Threats Introduced by Bring Your Own Devices (BYOD) Adoption in an Ethiopian Higher Educational Institution: Solutions to Security and Privacy

*Kibreab Adane**

The higher educational institutions of Ethiopia are seriously susceptible to cyber attacks. If malicious actors succeeded, it can adversely affect the security of sensitive information of stakeholders. The overall impact on security and privacy along with credibility of the institutions will be questioned. Usually, it is found that most of the organizations that encourage the culture of "Personal or Bring your Own Devices (BYOD)"are vulnerable to security and privacy breaches. The paper investigates and analyzes the security and privacy strategic considerations used by educational institutions when deciding the strategic adoption of BYOD. Further, the study finds out the cost-effective and secured solutions that can help these institutions balance the trade-offs between excessive-freedom of network access and protecting from BYOD security and privacy risks. The data was collected using interview of experts and a survey questionnaire to voluntary stakeholders. The findings reveal that BYOD is already in practice and adopted without considering transparent policies, security and privacy issues, device and application management tools, end-user security/privacy awareness and training. Also, there is excessive freedom of network access to whosoever is part of the network. This freedom causes security and privacy risks and bandwidth constraints. Finally, the study has made a comparative analysis of latest BYOD management tools using selected parameters like cost, diversified device and application management capability including device registration, remote tracking, wiping, locking and training/support from vendors for alleviating the issues and challenges. After critical analysis of mobile device management tools, the Manage Engine Mobile Device Manager (MEMDM) is proposed as the most fit software to meet the necessary criteria set.

***Keywords*:** BYOD, Security, Privacy, Higher education, Manage Engine Mobile Device Manager (MEMDM)

Introduction

When institutions of higher educational are susceptible to a cyber attack, its effects are loss of employee and students sensitive information. In such situations, operational, reputational and/or money-related impacts also become serious. This can hamper the national security and privacy (REMS, 2020). When a number of users access the higher educational institution's wireless network, their devices may not be guaranteed secure. It can make the higher education's network vulnerable (REMS, 2020). Among

* Faculty, Computing and Software Engineering, Arba Minch University, Arba Minch, Ethiopia. E-mail: Kibreab.adane@amu.edu.et

the major impacts; the sensitive information regarding student particulars, medical information and financial data can be stolen from these mobile devices, and hence educational institutions are said to be at risk of costly data security breaches (Kaseya, 2012; Durga and Sumit 2015; Vandna *et al.,* 2020; and Durga *et al.,* 2020).

Simply, Bring Your Own Device (BYOD) means allowing employees to access organization networks via their own devices/technology. This contributes to enhancing ease of work among employees and enhances their productivity. Among the significant challenges, security is one of the most important factors to be taken care of (Afreen, 2014).

As a matter of fact, the colleges and universities have seen a remarkable increase in the use of mobile devices in classroom learning practices (Faronics, 2020). Even though BYOD approach has cost effectiveness and usage benefits, it can bring some severe security threats. Also, it can have negative impacts on employee ethics and safeguards in framing company regulations (Dhingra, 2016).

It is noticeable that most organizations that encourage personal or BYOD may be prone to cyber security and privacy challenges. The security challenges found to be predominant in the universities include: user awareness, loss of device control, increased risk to organization's data and challenges of managing different BYOD devices and platforms. Evolving BYOD security challenges are dynamic and they keep on changing by the day. Establishing challenges due to BYOD adoption should not be a one-time activity but a continuous process. In addition, appropriate security measures should be put in place to mitigate the challenges (Sharma and Shekhawat, 2011; Sharma and Hardayal, 2012; Ounza *et al.,* 2018; and Verma *et al.*, 2018a).

The researcher approached one of the higher educational institutions in Ethiopia that encourages its students, staff and others to bring their own devices (BYOD) such as laptops, tablets, smartphones for accessing the university network. These diversified personal devices are allowed to access the university network with no restrictions applied to them. This indicates that endpoint security is neglected.

In general, it has been observed that the university networks are open for both university communities and non-university communities with excessive freedom of network access. Usually, there is no visible centralized BYOD device and applications management tool in these environments that can register BYOD devices, track, wipe, locks (stolen devices), restrict access to the university network if applications/software installed in personal devices are outdated as well as infected by malware. This loss of control and visibility over BYOD by the university's current network practices can be weak points and will open the door for hackers or malware. This can be an attempt to put the university network at security and privacy risks.

The main objective of the study is to investigate and analyze security and privacy considerations used by the university ICTs when deciding BYOD adoption. The

intention of the study is to find out the cost-effective and secured solutions that can help the university to balance the trade-offs between excessive-freedom of network access and protecting university assets from BYOD security and privacy risks.

The key aim of this study is to answer the following research questions:

- Which factors are considered by the university to decide BYOD adoption?
- What are enlisted security and privacy challenges faced due to BYOD adoption by the university ICTs?
- What are the security and privacy measures that have been put in place by the university to address the challenges due to BYOD adoption?

2. Literature Review

In order to find out the appropriate solution, the researcher rigorously reviewed the literature which uncovered the emphasis on factors that need to be considered when adopting an institution-wide BYOD strategy. These factors can be considered as relevant to higher educational institutions for balancing the trade-offs between excessive-freedom of network access and protecting university assets.

The main gaps in the reviewed literature are: (1) Authors recommended the Mobile Device Management (MDM) as BYOD management solution without considering the issues related to cost of device management tools; (2) Diversified personal device management capability; (3) Main security features of management tools; (4) Deployment (is it cloud-based or on-premise)?; (5) Do the vendors provide timely training or support?; and (6) Does it have a trial version? etc.

According to Woodbury (2013), when deciding the approaches to BYOD, there are a number of factors that should be considered for secured usages. These include: (1) What devices and who supports them; (2) Type of technology used for managing and securing mobile devices (e.g., MDM, Mobile Container Management (MCM), Mobile Application Management (MAM) and App Streaming); (3) The technology providers; (4) Privacy issues (i.e., If the device is lost or stolen); (5) What are your options to select? (allow employees to use their own devices but with restrictions applied to the phone, provide company-issued devices, forbidding the use of non-company-issued mobile devices for work-related tasks); and (6) Security policy (i.e., action taken against the device (and its contents – including personal data) when: the device is lost or stolen, the employee leaves the organization, the employee is terminated and the wrong security code to unlock the device is entered too many times).

After rigorous literature review, the factors identified for BYOD adoption in the higher learning institution were: security, infrastructure, cost (matters about cost implications or cost-effectiveness if BYOD is enabled), policy, privacy,

education (matters about educating users about BYOD policies, security and awareness), applications (the operating systems of the devices vary based on the devices used) (Sharma *et al.,* 2008; Vejayon *et al.*, 2016; Durga *et al.* 2016; and Verma *et al.,* 2018b).

Emery (2012) summarized 29 references from recognized academic and professional sources including peer-reviewed articles, reports, research theses and dissertations published between 2007 and 2012 and examined the following four selected aspects of an institution-wide BYOD strategy for higher education: (i) policy development: this includes statement of purpose, authorized uses, prohibited uses, system management and violation of policy; (ii) data security: includes segregate the data, require users to register their device, enable remote access to a mobile device, implement data encryption and use strong passwords; (iii) user education: includes training on (a) social media usage; (b) personally identifiable information; (c) strong password creation; and (d) privacy settings; and (iv) mobile-learning.

3. Materials and Methods

In order to achieve the objective of the study, the procedure given below is followed:

3.1 Study Area

The researcher selected the SNNPR region university ICTs in Ethiopia as study area for collecting the primary data. This is due to the fact that it has long experience in BYOD adoption. Additionally, due to the course work time constraints, the researcher did not include other universities.

3.2 Research Approach

Both quantitative and qualitative methods are used. Qualitative data analysis is used to validate the quantitative data.

3.3 Data Collection Instruments

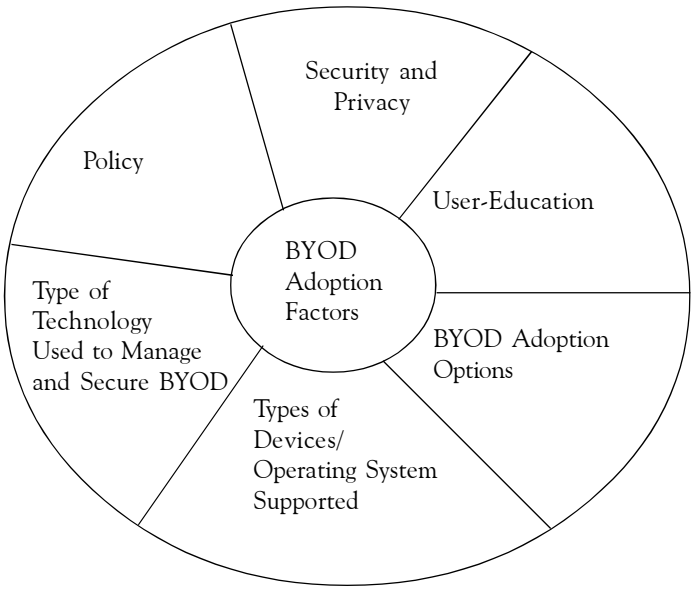
The data was collected through an interview with a sample of four (4) network administrators of the university and survey through distributing questionnaires to all instructors via university e-mail. As a sample, forty-two (42) volunteers/instructors appropriately filled the questionnaire (Appendix) and the data was analyzed over Google Form.

Moreover, based on the review of literature which provides emphasis on factors that need to be considered while adopting a higher- educational institution-wide BYOD strategy, the researcher prepared questionnaires and interviews that incorporated the following BYOD adoption factors, as indicated in Figure 1.

3.4 Tool Selection Method

Figure 2 shows how the fittest tools meet the necessary criteria selected.

Figure 1: BYOD Adoption Factors



3.5 Research Process Flow

Figure 3 shows the clear flow of the detailed research process.

4. Results and Discussion

4.1 Network Administrators Interview Result

The interview results obtained from network administrators are presented as follows:

4.1.1 Which Parameters/Factors Are Considered by the University to Decide BYOD Adoption?

In the interview, the network administrators of the university responded that BYOD is adopted inconsiderately of policies, BYOD device and application management tools as well as without the end-user security awareness and training. Within the current state of art practices, the foremost focus is simply on protecting the network infrastructure from external threats. However, internal threats coming from end-user sides and their personal devices have not been considered yet. For the long run, the responses revealed that they will have plans to contemplate it in phased manners.

4.1.2 What Are the Enlisted Security and Privacy Challenges Faced Due to BYOD Adoption by the University ICTs Due to BYOD Adoption?

The network administrator's responses clearly indicate that in the existing practice, the staff, students and whosoever is part of the network are allowed to access the

Figure 2: Tool Selection Method

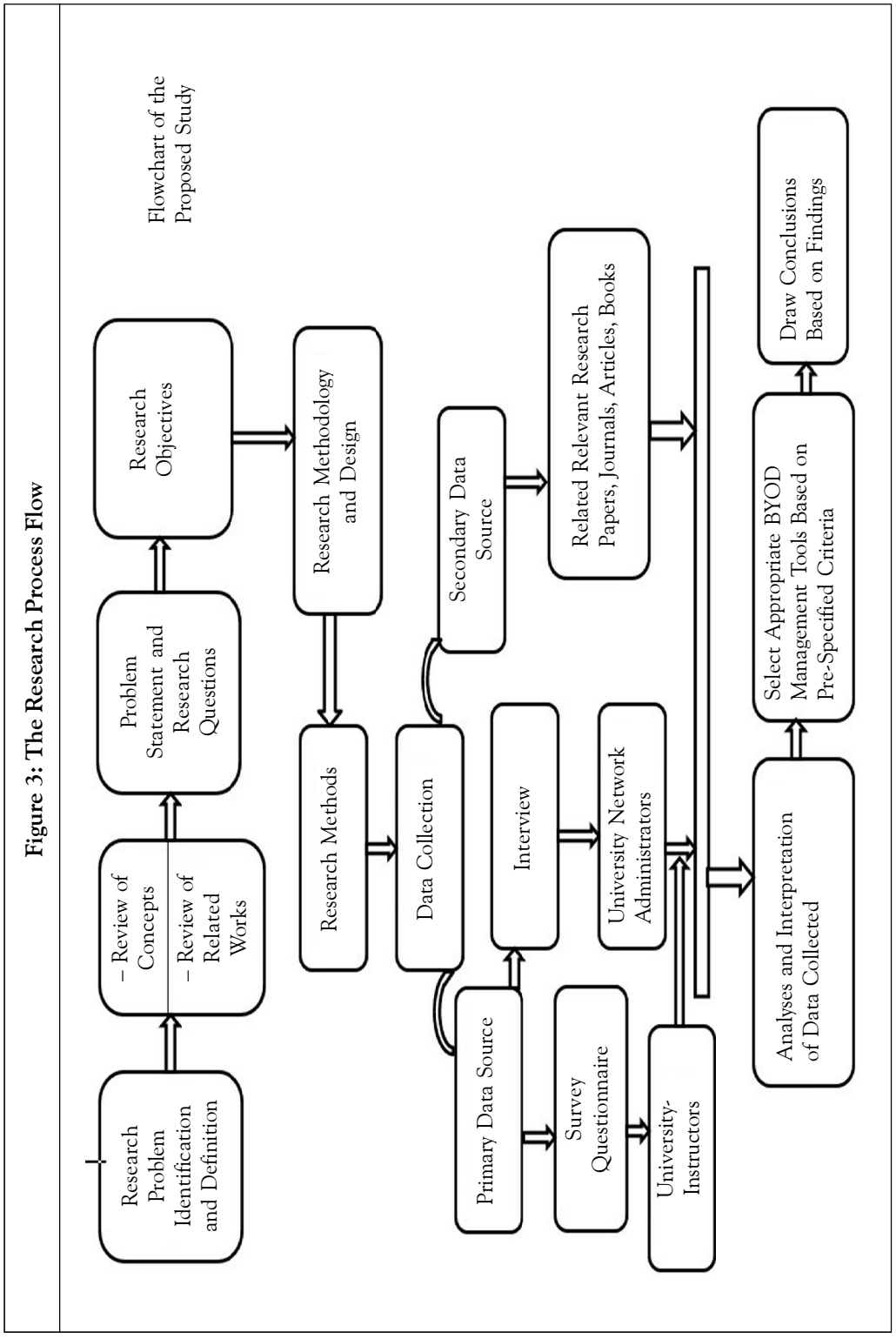


Figure 3: The Research Process Flow

university network using any device with undefined and unlimited freedom. Also, security and privacy risks as well as bandwidth constraints due to BYOD are neglected thoroughly. In the existing practices, no appropriate BYOD management tools are used in the university ICTs; there is a serious lack of visibility over personal devices especially over mobiles. It was revealed that the current technology does not have the capability of tracking, wiping, locking (if employee and students' devices are lost or stolen as well as if employee and students' devices and applications are vulnerable to malware and outdated). This implies that there is a strong need to have appropriate BYOD management tools in the university ICTs.

4.1.3 What Are the Security and Privacy Measures That Have Been Put in Place by University to Address the Challenges Due to BYOD Adoption?

The expert respondents' responses clearly revealed that there are no serious issues in security measures in the existing practices that have been put in place by the university ICTs. This will address the aforementioned challenges due to BYOD adoption. The target respondents clearly accepted that the future plan can have such strategies.

4.2 Volunteer/Instructors Survey Results

The questionnaire-based fact finding technique was used for survey of the volunteer/instructors from the university end users (Instructors). The respondents' mixed-ended responses are collected, categorized, analyzed and presented as follows:

4.2.1 Policies

Network admin group of the university clearly revealed that there is no BYOD policy in place. This shows a clear picture of the existence of an inappropriate BYOD adoption strategy. This implies that the university should have BYOD policies that can guide and administer the authorization, authentication and prohibition policies for the all types of users and stakeholders. When the policy violation is done by the users, then the BYOD policies should be considered for regulation and punishment. As represented in Figure 4, most of the respondents, i.e., 30 (71.4%) are not found to be aware of the university network usage policy in relation to their own devices, while only 12 (28.6%) respondents were found to be aware of the university network usage policy in relation to their own devices.

4.2.2 Security and Privacy

4.2.2.1 Password Handling

Figure 5 indicates that a majority of the respondents, i.e., 30(71.4%) use different passwords when they log into any of these accounts (e.g., e-mail/facebook/your device/Student Management System (SMIS), while 12 (28.6%) respondents responded that the same password is used by them for different accounts. Thus, using the same password for different accounts is not recommended due to the fact that if the hacker compromised the security measures and hacked a single account, it is very easy for him/her to hack the rest of the accounts.

Figure 4: Respondents' Awareness About the University Network Usage in Relation to Their Personal Devices

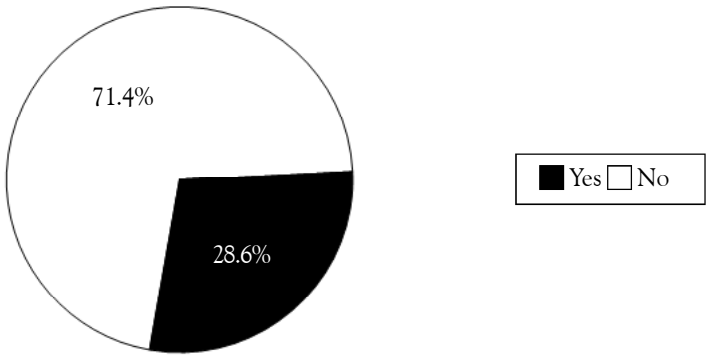


Figure 5: Whether Respondents Use the Same or Different Passwords for Different Accounts

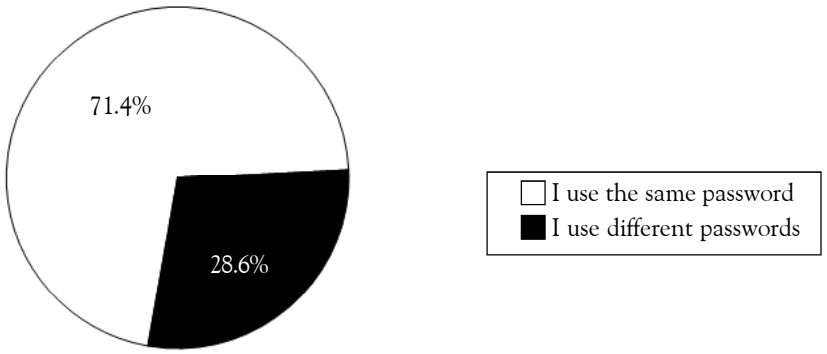
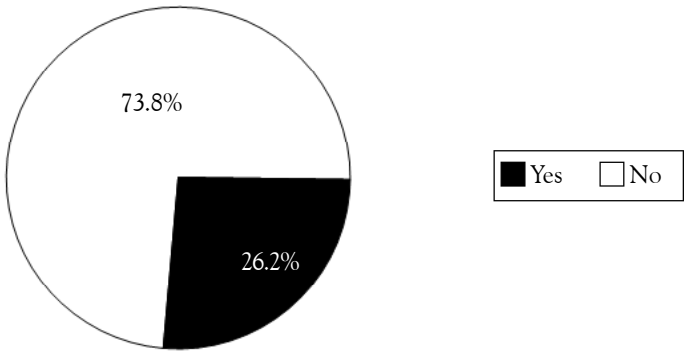


Figure 6 indicates that a majority, i.e., 31 (73.8%) of respondents revealed that they never shared their password with anyone known, while only 11(26.2%) of them

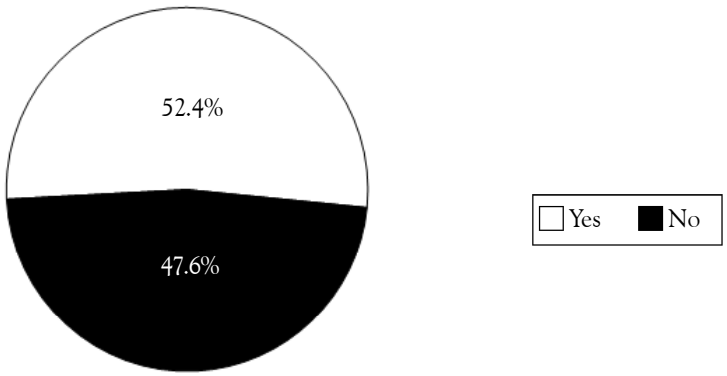
Figure 6: Whether Respondents Ever Shared Their Password with Someone



shared their passwords. A common practice of sharing the passwords has been considered as poor handling and management policy of passwords and serious violation of security measures. These challenges can be alleviated through adequate training to the users.

Further, all the information stored in users' personal devices may not have equal importance; however, protecting most sensitive information likes exams, photos, contacts, SMS, financial information, medical information and so on is of vital importance. Figure 7 indicates that more than half of the respondents, i.e., 22(52.4%) revealed that they do not have password-protected files or folder on their personal devices, while only 20(47.6%) of them have password-protected files or folder on their personal devices.

Figure 7: Whether Respondents Have Password-Protected Files or Folders on Their Personal Devices



4.2.2.2 E-mail

Figure 8 indicates that a majority of the respondents, i.e., 30 (71.4%) responded that they received an e-mail link from unknown sources, while only 12 (26.8%) of them did not receive an e-mail link from any unknown source.

It is important to note that clicking the e-mail link received from an unknown source without identifying and verifying the source can bring harm to user files and systems. This is due to the fact that the link may contain malicious code that can be downloaded to user devices. Figure 9 shows that among the respondents who received e-mail link from unknown sources, only a few respondents, i.e., 8 (25.8%), performed the identification and verification of the source before clicking the e-mail link, while 10 (32.3%) of them clicked a link and checked the e-mail content without identification and verification of the source. There were also respondents who ignored the clicking and checking of the e-mail content received from an unknown source, i.e., 14 (41.9%).

Figure 8: Whether Respondents Ever Received an E-mail from Unknown Sources

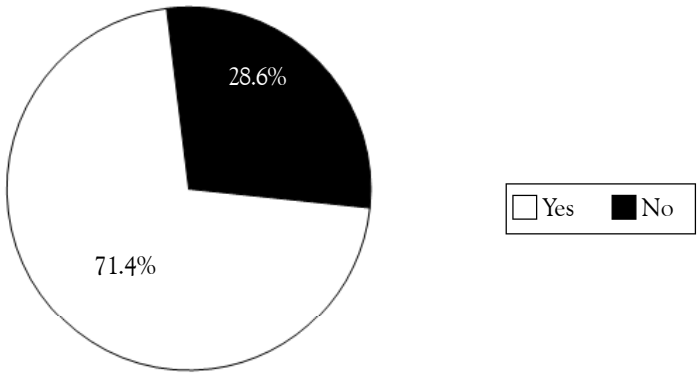
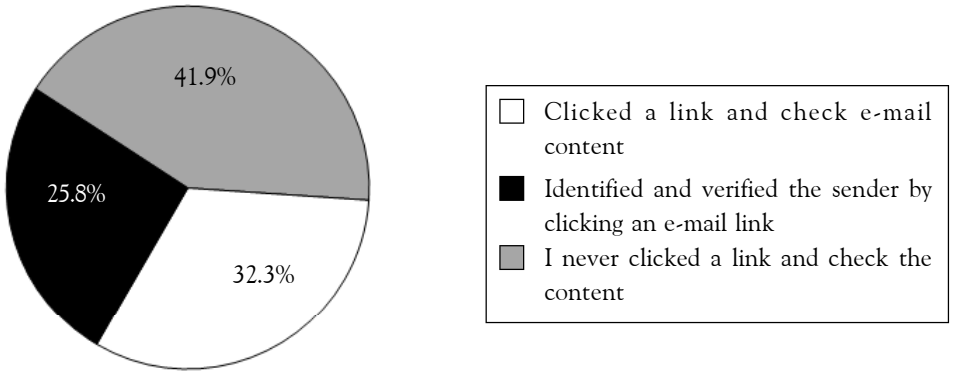


Figure 9: Whether Respondents Took Action When They Received an E-mail from Unknown Sources

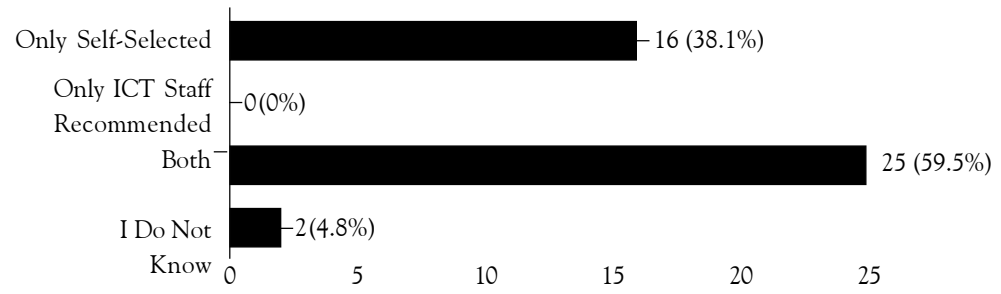


4.2.2.3 Application

The findings clearly revealed that the university's ICT does not have BYOD management software. This implies that any user can access the university network through insecure devices and there are higher levels of possibilities for cyber attacks.

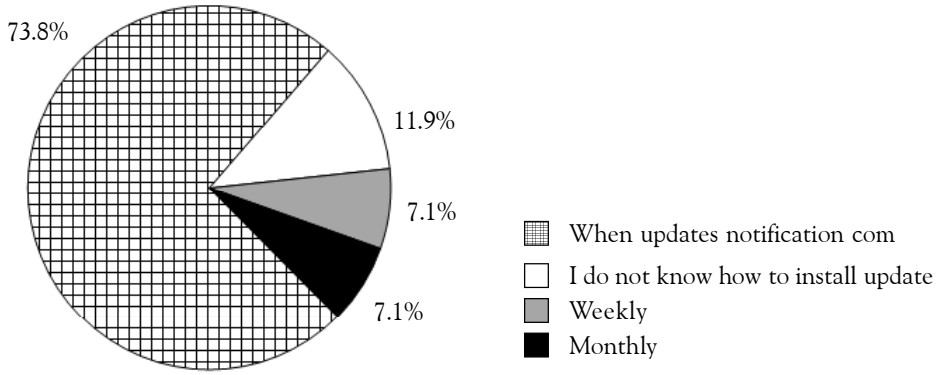
In order to enhance the security, it is recommended to follow the ICT expert advisories and related applications/software. This is due to the fact that downloading software/applications from malicious sites can also be a dangerous phenomenon which can harm the sensitive files. Figure 10 clearly indicates that a majority of the respondents, i.e., 25 (59.5%) use both self-selected and university ICT recommended applications/software, while only 16 (38.1%) of them accepted only self-selected applications/software. The rest, 2 (4.8%) of them, accepted that they neither use and nor are aware of such kinds of precautionary measures, tools and techniques.

Figure 10: Whether Respondents Are Self-Selected or University ICT Staff or Recommended



As indicated in Figure 11, a majority of the respondents, i.e., 31 (73.8%) install application/operating system updates on their devices when update notification appears. There are also respondents who do not know how to install updates which accounts for 5 (11.9%), while 3(7.1%) of them install updates weekly and monthly. Special training is required for those who do not know how to install updates.

Figure 11: How Often Respondents Installed Application/OS Updates

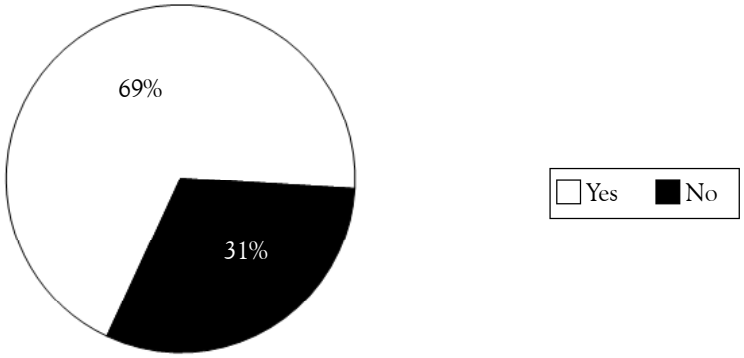


4.2.2.4 Stolen Devices

Even though the tracking, wiping and locking of the stolen devices need technological solutions, the university ICT lacks the technology that has such capability. As Figure 12 indicates, a majority of respondents, i.e., 29(69%) never lost their device due to theft, while only 13 (31%) of them lost their devices due to theft.

The respondents who lost their devices were asked where they reported when their devices were lost. A majority, i.e., 69.2% of them had not reported to any one,

Figure 12: Whether Respondents Had Lost Their Personal Devices (i.e., Laptop, Mobile and Tablet) Due to Theft

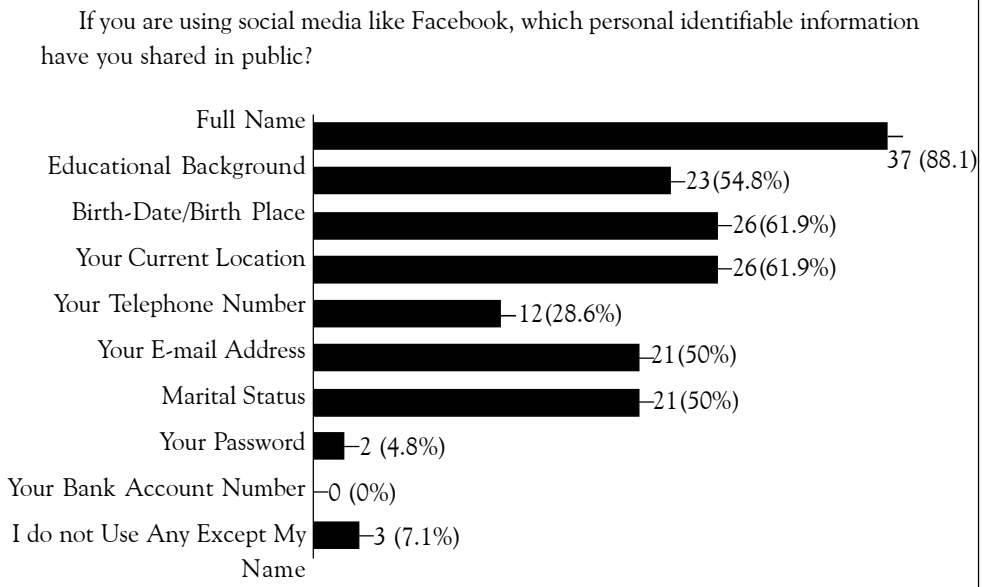


while 30.8% of them reported to the police. This indicates that there is no technological means used by the respondents to track their stolen devices.

4.4.2.5 Social Media Usage

Figure 13 shows that the respondents' current trend is to share, not to protect. A majority of respondents share their private information on public social media. This implies that a high level of possibility exists for social engineering or hackers to commit crime through misuse of their sensitive information.

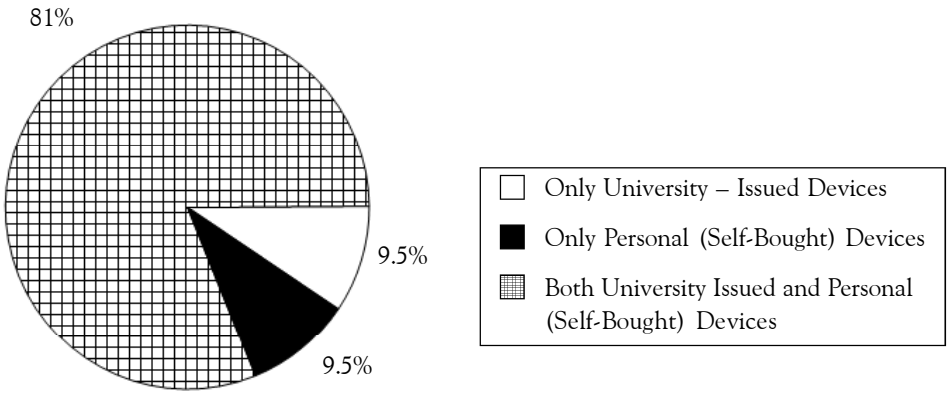
Figure 13: Social Media Usage by Respondents



4.3 Types of Devices /Operating System Used

The findings reveal that the university issued devices and the personal devices are allowed to access the network. Figure 14 shows that a majority of the respondents, i.e., 34 (81%) used both university issued device and the personal device to access the university network; and only 4 (9.5%) of them used personal devices and the remaining 4 (9.5%) used only university issued devices.

Figure 14: Whether Respondents Use the University Issued or Personal Devices to Access the Network



In order to find out the suitable BYOD management software, it is important to know the type of devices/operating systems used by respondents to access the university network. Figure 15 shows that a majority of the respondents, i.e., 32 (76.2%) used the android mobile, 31 (73.8%) laptop with Windows Operating System, 6 (14.3%) tablet, 3 (7.1%) Apple (IOS) and 1 (2.4%) of them others.

This finding implies that there is a strong need for diversified personal device management software by the university ICT to have visibility over the devices, as given in Figure 15.

When a question was asked about the accessibility of the university network, as Figure 16 shows, a majority of respondents, i.e., 37 (88.1%) responded that they use it daily over their personal devices, while 4 (9.5%) once in a week, and 1 (2.4%) of them accessing twice a week.

4.4 Education

The findings clearly indicate that there is existence of a critical gap in IT security and privacy. They accepted that they need continuous awareness and training sessions. The research identified the following knowledge gaps that need special attention for training and awareness:

Figure 15: What Type of Personal Devices Respondents Use

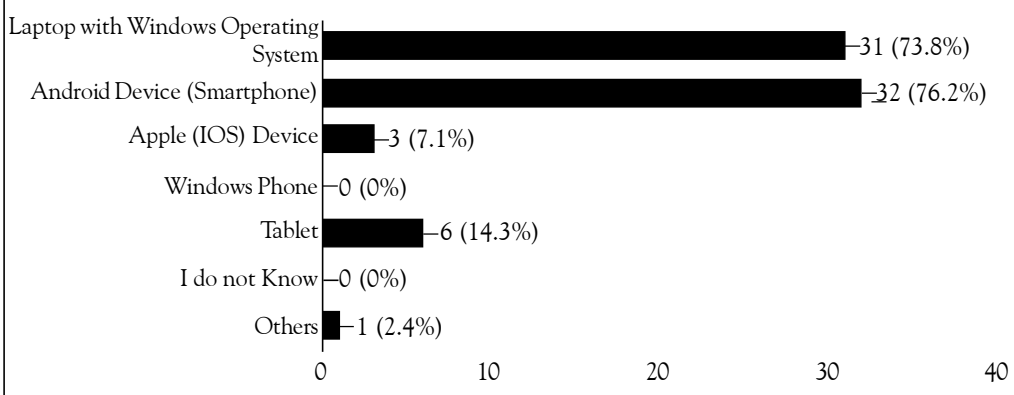
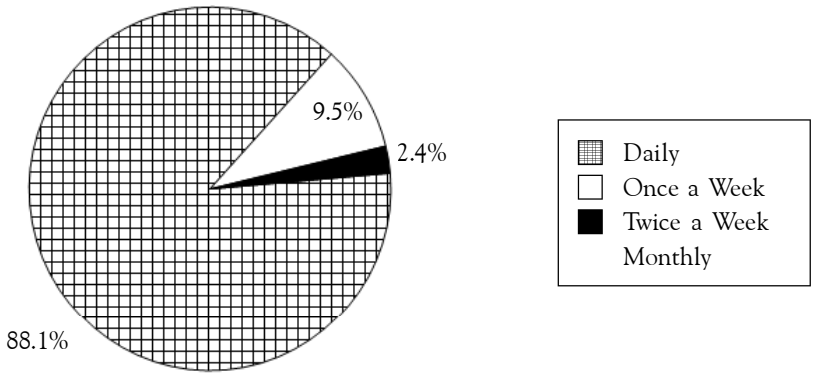


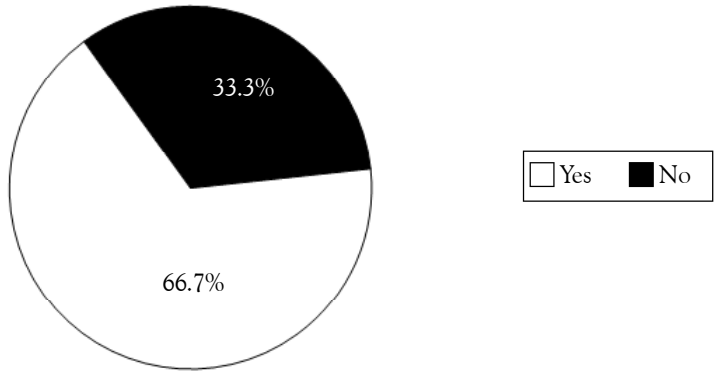
Figure 16: How Often Respondents Access the University Network Through Their Personal Devices



- Sharing their passwords with others;
- Clicking an e-mail link received from unknown sources;
- Do not know how to update applications/operating system installed on their devices;
- Sharing sensitive information like password, e-mail, telephone, location information, birth date on social media;
- Exposed to computer viruses;
- Not having password-protected files or folders in their personal devices; and
- Using non-IT expert recommended applications and software.

Figure 17 shows that a majority of the respondents, i.e., 28 (66.7%) found feeling secured when using the university network over their own devices. However, 14 (33.3%) of them were not feeling secured, while using the university network over their own devices. The respondents revealed the following important factors which can make them not to feel secured: (1) the ICT staff can access their personal data available in their device; (2) ICT computers have more viruses; (3) SMIS account is accessed by higher officials by resetting passwords.

Figure 17: Whether Respondents Feel Secure While Using the University Network



Thus, there should be transparency and accountability for highly privileged admins who have deliberate unauthorized access to respondents' accounts. This is an unethical act that makes the users feel not secured and resistance to use the university network.

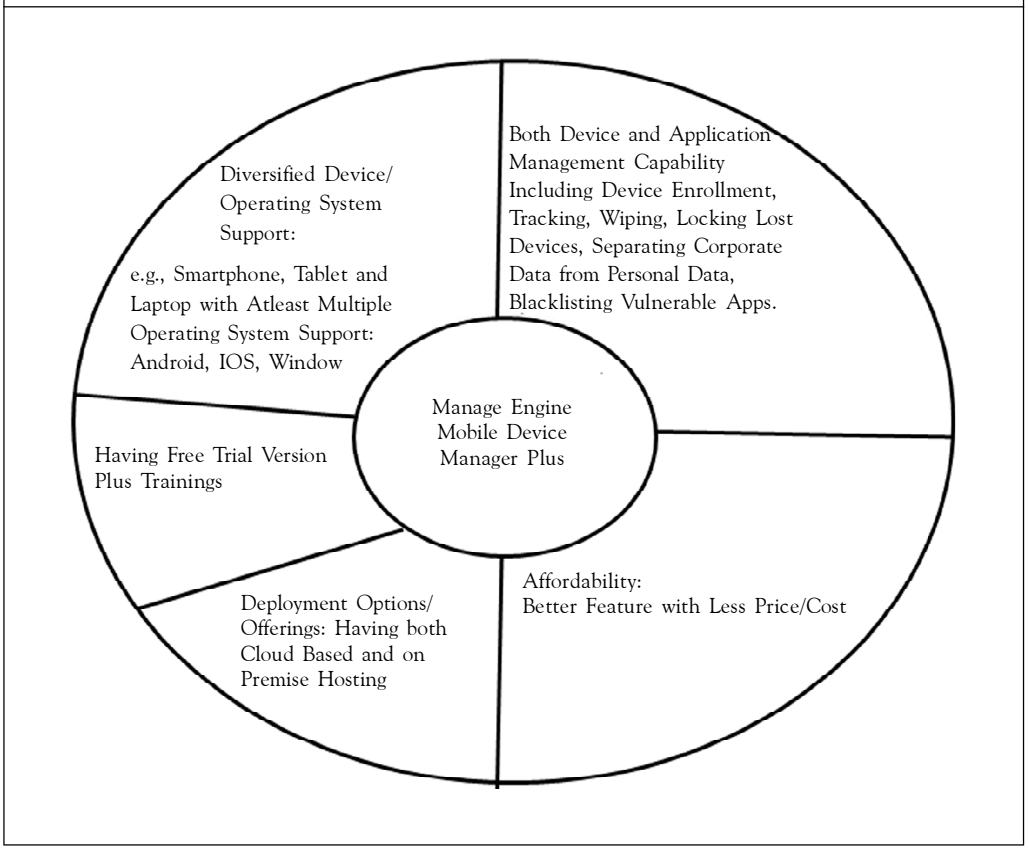
4.5 Proposed Solution

In order to suggest a suitable solution, the researcher understands the problems in the existing system; then proceed for a comparative analysis of latest BYOD management tools using selected parameters/factors like cost, diversified device and application management capability including device registration, remote tracking, wiping, locking (stolen devices), having both cloud and on-premise-based offerings and training/support from vendors for alleviating the issues and challenges. After critical analysis of the MDM tools, the Manage Engine Mobile Device Manager (MEMDM) is proposed as the fit solution to meet the necessary criteria set.

Figure 18 shows the proposed MDM tool selection methods. Figure 19 shows the criteria for choosing MEMDM plus. Moreover, what makes the MEMDM cost-effective is that it offers to manage for free up to 25 devices, and it costs $10/device/year, if it is more than 25 devices.

Figure 18: Criteria for Choosing Cost-Effective and Secured MDM Tools

Figure 19: Criteria for Choosing Manage Engine Mobile Device Manager Plus



Conclusion

In order to secure the university network and provide quality services to users, it is important to control the inappropriate activities and focus on productivity. Unless the university allows proper utilization of the university network through personal devices, the security and privacy risks as well as bandwidth constraints become more challenging. The findings reveal that BYOD is already in practice and adopted without considering transparent policies, security and privacy issues. Also, the device and application management tools, end-user security/privacy awareness and training are also not up to the mark. There is excessive freedom of network access to whosoever is part of the network and this poses a serious security risk.

Due to the lack of suitable BYOD management tools, the network admins are unable to visualize and manage diversified personal devices. To find out the latest, cost-effective and secured BYOD management solutions, the paper has made a comparative analysis of latest BYOD management tools using selected parameters. After critical analysis of MDM tools, the MEMDM is proposed as the most fit software to meet the necessary criteria set.

Moreover, to safeguard the security and privacy of the university network, the university should not only focus on technological options but also narrow the knowledge gaps of users especially in password handling, e-mail usage, software downloading/ updating as well as social media usage by providing continuous training and through awareness creation.

References

1. Afreen (2014), "Bring Your Own Device (BYOD), in Higher Education: Opportunities and Challenges", Provided by *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, available at https://www.researchgate.net/publication/261136229_Bring_Your_Own_ Device_BYOD_in_ Higher_ Education_Opportunities_and_Challenges
2. Dhingra (2016), "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)", *Procedia Computer Science*, Vol. 78, pp. 179-184.9, Elsevier, available online at www.sciencedirect.com/82446305.pdf.
3. Durga Prasad Sharma and Sumit Gautam (2015), "Radio Frequencies Spectrum Auction of 2015 and its Impact on Indian Mobile Service Providers", *Suresh Gyan Vihar University International Journal of Environment, Science and Technology*, available at http://www.gyanvihar.org/researchjournals/19.pdf
4. Durga Prasad Sharma, Rakesh Kumar Sharma and Alade Ayodele J (2016), "Context Aware Inter-System Radio Connections Management to Improve User Experience in Voice over Wi-Fi Solution", *International Journal of Research and Analytical Reviews (IJRAR)*, available at www.ijrar.org
5. Durga Prasad Sharma, Kasaye Asres and Amin Tuni Gure (2020), "Automatic Surveillance and Control System Framework-DPS-KA-AT for Alleviating Disruptions of Social Media in Higher Learning Institutions", *Journal of Computer and Communications*, Vol. 8, No. 1, pp. 1-15 Scientific Research Publishing, USA.
6. Emery (2012), "Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education", Continuing Education 1277 University of Oregon Eugene, Applied Information Management Program, pp 1-111, available at olarsbank.uoregon.edu.
7. Faronics (2020), "Managing Mobile Devices in Higher Education", available at https://www.faronics.com/assets/Managing-Mobile-Devices-in-Higher-Education.pdf. Accessed on February 3, 2020.
8. Kaseya (2012), Three Key Mobile Device Management and Security Steps Educational Institutions Should Focus on: https://www.kaseya.com/blog/2012/07/19/mobile-device-management-and-security-for-colleges-universities/
9. Ounza J E, Liyala S and Ogara S (2018), "Emerging Security Challenges due to Bring Your Own Device Adoption: A Survey of Universities in Kenya", *International Journal of Science and Research (IJSR)*, Vol. 7, No. 1, pp. 345-349.

10. Readness and Emergency Management for Schools (REMS) (2020), Technical Assistance (TA) Center, Cyber Security for Higher Ed Fact Sheet, available at https://rems.ed.gov/docs/Cybersecurity_Considerations_ for_Higher_ed_Fact_ Sheet_508C.pdf. Accessed on February 25, 2020.

11. Vejayon J, Samy G N, Maarop N *et al.* (2016), "Adopting Factors of Bring your Own Device (BYOD) at the Selected Private Higher Learning Institution in Malaysia", *Journal of Advanced Research in Social and Behavioural Sciences,* Vol. 2, No. 1, pp. 24-32.

12. Verma V R, Sharma D P and Lamba C S (2018a), "Stable Energy Proficient and Load Balancing Based QoS Routing in Mobile Ad-Hoc Networks: Mobile Software Based Approach", *Malaya Journal of Matematik (MJM)*, University Press, available at http://www.malayajournal.org/articles/MJM0S0115.pdf

13. Verma V R, Sharma D P and Lamba C S (2018b), "Expansion in Quality of Service of MANET during Route Determination Phase by Mobile Software Agent Approach", *International Journal of Applied Engineering Research*, available at https:/ /www.ripublication.com/ijaer18/ijaerv13n15_29.pdf

14. Sharma D P and Hardayal Singh Shekhawat (2012), "Hybrid Cloud Computing in e-governance: Related Security Risks and Solutions", *Research Journal of Information Technology*, Vol. 4, No. 1, pp. 125-130.

15. Sharma D P and Shekhawat N S (2011), "Cloud Computing Security Through Cryptography for the Banking Sector", Proceedings of the 5th National Conference, SCOPUS Publication-India, available at http://www.bvicam.ac.in/news/INDIA Com%202011/258.pdf

16. Sharma D P, Sharma R K and Ayodele A J (2008), "Convergence of Intranetware in Project Management for Effective Enterprise Management", *Journal of Global Information Technology (JGIT)*, Vol. 4, No. 1, pp. 54-74.

17. Vandna Rani Verma, Sharma D P and Lamba C S (2020), "Performance Improvement in MANET Routing by Paradigm Shifting Through Mobile Agent Approach", available at SSRN 3574033.

18. Woodbury (2013), Security and Privacy Considerations for BYOD, ©SkyView Partners, Inc. All Rights Reserved, available at: http://www.ozglobal software.com/ downloads/Security-and-Privacy-Considerations-for-BYOD.pdf

Appendix

Questionnaire		
Policy		
1. Do you have BYOD adoption policy in place?	Yes	☐
(For Network Administrators)	No	☐
2. Does University ICT staff made you aware of the university network usage policy in relation to your own devices?	Yes	☐
	No	☐
Password Handling		
3. Are you using the same password or different passwords while you are logging into any two of these accounts (e.g., e-mail/ Facebook/your device/Student Management system (SMIS))?		
I use the same password		☐
I use different passwords		☐
4. Have you ever shared your password to some one?	Yes	☐
	No	☐
5. Is there password-protected files or folder in your personal devices? (Mobile, Tablet and Laptop)	Yes	☐
	No	☐
E-mail Usage		
6. Have you ever received e-mail link from unknown source(s)?	Yes	☐
	No	☐
7. If you ever received e-mail link from unknown source(s), specify action you have taken to that e-mail link?		
Clicked a link and check e-mail content		☐
Identified and verified the sender by clicking an e-mail link		☐
I never clicked a link and check the content		☐
Application Usage		
8. The applications/software installed in your device(s) is self-selected or University ICT staff recommended or both or not sure?		
Only self-selected		☐
Only ICT staff		☐

Appendix (Cont.)

Recommended both		☐
I do not know		☐
9. How often do you install application/operating system updates on your devices?		
When updates notification on		☐
I do not know how to install update		☐
Weekly		☐
Monthly		☐
Stolen Devices		
10. Have you ever lost your device due to theft?	Yes	☐
(Mobile, Tablet and Laptop)	No	☐
11. If you ever lost your device due to theft, to whom you report after theft?		
_____		
Social Media Usage		
12. If you are using social media like Facebook, which personal Identifiable Information have you shared in public? Tick any that apply:		
Full name		☐
Educational background		☐
Birth-date/birth place		☐
Your current location		☐
Your telephone number		☐
Your e-mail address		☐
Marital status		☐
Your password		☐
Your bank account number		☐
I do not use any except my name		☐

Appendix (Cont.)

Types of Devices/Operating System Used

13. Are you using university-issued or personal (self-bought) devices to access university network?

- Only university-issued devices ☐
- Only personal (self-bought) devices ☐
- Both university-issued and personal (self-bought) devices ☐

14. What type of personal devices you use to access the university network?

- Laptop with Windows Operating System ☐
- Android device (smartphone) ☐
- Apple (IOS) device ☐
- Windows phone ☐
- Tablet ☐
- I do not know ☐
- Others ☐

15. How often do you use your own devices to access the university network?

- Daily ☐
- Once a week ☐
- Twice a week ☐
- Monthly ☐

Security Education/Training

16. What are the knowledge gaps of respondents in IT security and privacy that needs special attention for training and awareness

_____

17. Do you feel secured while using university network by your own devices? Yes ☐ No ☐

Reference # 35J-2020-06-01-01