Model Tahap Kesedaran Pekerja Terhadap Penggunaan BYOD di Sektor Awam

Wan Yuswani bin Wan Jusoh
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsan Malaysia
yuswani.jusoh@gmail.com

Ibrahim bin Mohamed
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
ibrahim@ukm.edu.my

ABSTRAK

BYOD atau penggunaan peranti mudah alih peribadi seperti telefon pintar dan tablet di pejabat meningkatkan produktiviti serta memudahkan pengguna dalam melakukan tugas seharian dengan mengakses data organisasi mahupun data peribadi menggunakan rangkaian dalaman jabatan. Kurangnya kesedaran dan ciri-ciri keselamatan terhadap penggunaan peranti BYOD boleh mengakibatkan kebocoran data, ancaman kepada integriti maklumat, peranti hilang atau dicuri, meningkatkan risiko kehilangan data sensitif dan boleh mengakibatkan ancaman serangan penyebaran malware ke dalam rangkaian jabatan. Jesteru, kesedaran pekerja terhadap penggunaan peranti BYOD amat penting bagi mengelak berlakunya insiden keselamatan. Kajian ini bertujuan mengenal pasti tahap kesedaran pekerja terhadap penggunaan peranti BYOD di sektor awam yang melibatkan kakitangan Unit Penyelarasan dan Pelaksanaan, Jabatan Perdana Menteri (ICU JPM) sebagai kajian kes. Bagi mengukur tahap kesedaran pekerja terhadap penggunaan BYOD, kaedah model faktor kesedaran digunakan untuk mengukur faktor yang berkait rapat dengan manusia, proses dan teknologi. Pendekatan kajian adalah gabungan kaedah kualitatif melalui temu bual bagi penentusahan model bersama pakar dan kuantitatif bagi mengukurkan tahap kesedaran responden terhadap BYOD dan membentuk model kajian ini melalui kaji selidik. Hasil dapatan mendapati indeks kebolehpercayaan setiap komponen soalan kaji selidik adalah baik dan cemerlang dengan nilai *Cronbach's Alpha* di antara 0.803 – 0.944. Menerusi ujian skor min, nilai yang diperolehi untuk setiap komponen adalah tinggi di antara 5.45 – 6.43. Menerusi ujian analisis faktor, data di analisis menggunakan analisis komponen prinsipal dan data kemudiannya diputar dengan mengunakan pusingan *varimax*. Hasil keseluruhan komponen formaliti dan simpanan dijadikan model akhir Tahap Kesedaran Pekerja Terhadap Penggunaan BYOD di Sektor Awam.

Kata kunci—Bring Your Own Device (BYOD); kesedaran maklumat; keselamatan maklumat

1. PENGENALAN

Kemajuan teknologi yang semakin pesat telah menggalakkan industri pengkomputeran menghasilkan produk yang lebih kompak, ringan dan fleksibel. Tambahan pula tuntutan globalisasi memerlukan urusan perniagaan secara atas talian mengghairahkan lagi penghasilan peralatan mobil untuk mudah dibawa bersama ke mana jua. Oleh yang demikian, konsep Membawa Peranti Anda Sendiri (MPAS) atau juga dikenali sebagai *Bring Your Own Device* (BYOD) menjadi pilihan masa kini [1].

BYOD merupakan satu konsep atau dasar di mana organisasi membenarkan para pekerjanya membawa peralatan mudah alih persendirian untuk melaksanakan tugasan rasmi di pejabat melalui sambungan rangkaian Jabatan / Kementerian. Dasar ini juga membenarkan pekerja untuk mencapai data organisasi melalui peranti mobil mereka [2]. Peralatan mobil yang dimaksudkan seperti komputer riba, telefon pintar, tablet dan komputer peribadi. Peranti ini dilengkapi dengan pelbagai kegunaan seperti melayari internet, perkhidmatan e-mel, memindahkan fail, melakukan transaksi atas talian melalui aplikasi berasaskan web dan sebagainya. Peralatan ini bukan sahaja boleh digunakan di pejabat malah mudah dibawa ke mana sahaja seperti bertemu pelanggan, menghadiri kursus dan membentangkan kertas kerja di luar organisasi. Semua perkhidmatan ini membenarkan pengguna untuk mengakses data atau maklumat pada persekitaran tempat kerja dan bekerjasama di antara satu sama yang lain [3].

Kajian [4], menganggarkan ada lebih daripada satu bilion peranti BYOD digunakan di tempat kerja di seluruh dunia pada 2018. Satu lagi kajian oleh [2], mendapati bahawa 95% peserta menggunakan peranti mereka sendiri untuk melaksanakan fungsi kerja. Angka-angka semakin bertambah dan kian meningkat kerana BYOD memberikan manfaat kepada organisasi itu sendiri. [3] menyatakan bahawa BYOD bermanfaat kepada pekerja. Ianya meningkatkan produktiviti pekerja, meningkatkan kecekapan prestasi, memberikan kemudahan serta kepuasan kepada pekerja pada persekitaran fleksibiliti dan mobiliti.

Trend BYOD secara beransur-ansur menjadi popular di dunia perniagaan hari ini kerana ianya menawarkan banyak kelebihan kepada majikan dan pekerja. Sebagai contoh, jika pekerja

membawa peranti mereka sendiri (komputer riba atau telefon pintar), maka mereka tidak perlu membawa peranti yang disediakan oleh majikan untuk bekerja dan dengan ini bebanan mereka dapat dikurangkan. BYOD juga meningkatkan produktiviti dan inovasi kepada pekerja kerana mereka akan merasa lebih selesa menggunakan peranti sendiri. Dari sudut organisasi pula, ianya memberi manfaat kepada majikan kerana majikan tidak perlu mencari, membeli dan memasangnya, di mana akan dapat mengurangkan kos penyelenggaraan struktur IT [5]. Para pekerja juga lebih puas apabila menggunakan peranti mereka sendiri dan bukan peranti yang dikeluarkan oleh firma mereka [6].

Hasil kajian menunjukkan 84% organisasi menggalakkan amalan BYOD manakala hanya 16% organisasi masih belum bersedia membenarkan amalan BYOD ke dalam organisasi [4]. Namun demikian, langkah organisasi membenarkan pekerja membawa peranti sendiri bukan pilihan yang bijak untuk organisasi itu sendiri. Kajian [6], membenarkan BYOD di dalam sesebuah organisasi itu menimbulkan beberapa implikasi buat organisasi dan pekerja dari pelbagai aspek termasuk kos IT dan keselamatan mobiliti secara berterusan. Terdapat banyak risiko yang berkaitan dengan penggunaan peranti peribadi di tempat kerja. Sebagai contoh penggunaan peranti peribadi di tempat kerja mengundang pelbagai cabaran keselamatan untuk organisasi di seluruh dunia.

Pelaksanaan BYOD telah mengundang pelbagai masalah jenayah siber contohnya penggodam boleh mencuri data maklumat peribadi atau menyelinap masuk ke dalam data perbankan dan mencuri wang mereka. Dengan peningkatan penggunaan peranti mudah alih ini menyebabkan berlakunya kebocoran maklumat dan keselamatan data melalui peranti mudah alih tersebut [7]. Terdapat pelbagai cabaran bagaimana untuk menjamin informasi dan maklumat yang terkandung di dalam peranti mudah alih ini tidak bocor jika peranti tersebut hilang, kecurian atau telah disalahgunakan oleh pihak-pihak yang tidak bertanggungjawab [8].

Kerajaan Malaysia melalui Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) telah mewujudkan satu dokumen garis panduan Dasar Keselamatan ICT (DKICT) MAMPU pada tahun 2010. Menerusi garis panduan tersebut, Unit Penyelarasan dan Pelaksanaan, Jabatan Perdana Menteri (ICU JPM) telah meminda dan mengeluarkan DKICT ICU

JPM versi 5.3 pada tahun 2016 yang mencakupi penggunaan BYOD di ICU JPM bagi meminimumkan kesan insiden keselamatan ICT, melindungi kerahsiaan data maklumat ICT, integriti, kebolehsediaan dan penyalahgunaan peranti mudah alih di pejabat [9].

Kajian ini dilakukan setelah melihat serta mengkaji berdasarkan keperluan semasa yang mendesak tentang penggunaan peranti BYOD di sektor awam. Kesedaran pekerja terhadap penggunaan peranti BYOD perlu dipupuk oleh setiap pengguna peranti BYOD. Penggunaan peranti BYOD pada masa kini dianggap satu keperluan dan ianya memudahkan dan mempercepatkan tugas-tugas harian di samping ianya dapat meningkatkan kecekapan, produktiviti serta mutu kerja. Ciri-ciri keselamatan yang sepatutnya perlu dititikberatkan semasa penggunaan peranti BYOD bagi mengurangkan risiko kehilangan data dan kebocoran maklumat.

2. KAJIAN BERKAITAN

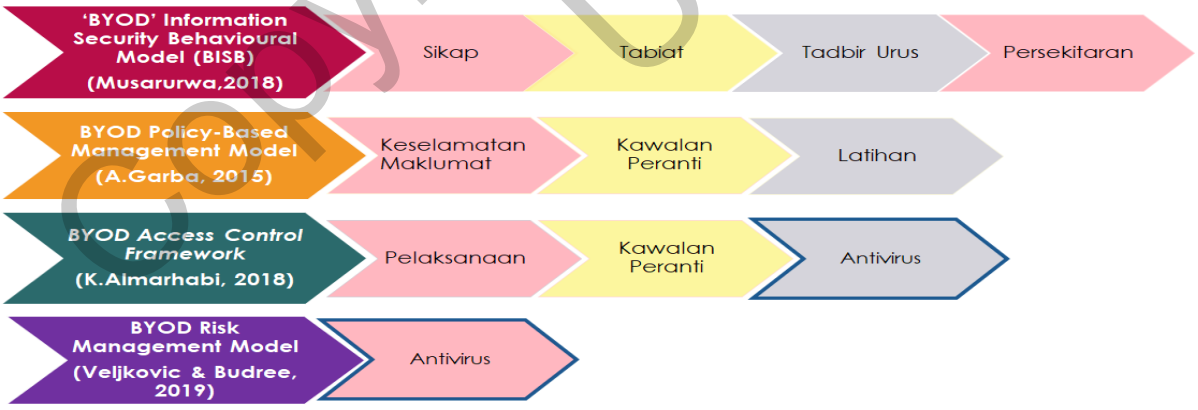
[10] berkata, penggunaan BYOD membantu para pekerja dalam melaksanakan tanggungjawab tanpa mengira masa dan tempat. BYOD boleh didefinisikan sebagai strategi yang membolehkan pekerja, rakan niaga dan pengguna lain menggunakan peranti yang dipilih dan dibeli secara peribadi untuk mengguna pakai sistem aplikasi organisasi dan mengakses data [11]. Fenomena penggunaan BYOD yang semakin meluas adalah salah satu hasil daripada bidang perniagaan yang dilakukan secara dalam talian. Sebilangan perspektif mengenai kemunculan BYOD dalam organisasi dilihat dalam beberapa kajian lepas. Perspektif pertama ialah BYOD adalah konsep yang digunakan oleh pekerja dalam memastikan mereka dapat melakukan bebanan tugasan yang semakin banyak dalam memastikan proses perkhidmatan organisasi dan kehendak pengguna dipenuhi [12].

Perspektif kedua adalah organisasi melihat faedah dalam membenarkan peranti milik peribadi mengakses sumber IT yang seterusnya mendorong kepada kecekapan dan proses penambahbaikan proses perkhidmatan [13][14]. Perspektif lain menunjukkan bahawa perkembangan konsep BYOD sebagai konsep saling menguntungkan, dengan kedua-dua pihak di antara majikan dan pekerja [15]. Para penyelidik melihat konsep BYOD dapat mengurangkan kos operasi dalaman melalui pengurangan keperluan bagi ruang pejabat, perkakasan dan sistem

telefon. Organisasi juga melihat terdapatnya peningkatan produktiviti pekerja. Dengan menggunakan kaedah pengukuran yang dikembangkan dalam penulisan-penulisan sebelumnya yang berkaitan dengan BYOD, hasil kajian mendapati bahawa peningkatan atau penurunan kualiti dan kuantiti pekerjaan dilakukan. Pekerjaan yang efektif serta efisien dapat diukur hasil daripada penggunaan teknologi mudah alih [16].

Pembangunan model awal kajian ini berdasarkan persoalan kajian dan objektif kajian yang hendak dicapai. Persoalan kajian pertama tertumpu kepada mengenal pasti aspek dan faktor yang mempengaruhi tahap kesedaran pekerja terhadap penggunaan BYOD.

Menurut [17] telah mencadangkan sifat tingkah laku melalui model BYOD Information Security Model (BISB) yang menitikberat mengenai faktor sikap, tabiat, tadbir urus dan persekitaran. [2] pula melalui cadangan BYOD policy-based management model mengesyorkan makanisma komponen kawalan merangkumi faktor keselamatan maklumat, kawalan peranti dan latihan. Manakala [18] telah menekankan faktor pelaksanaan kawalan polisi serta kawalan peranti bagi menguatkuasakan polisi penggunaan peranti BYOD di tempat kerja. Oleh yang demikian, pemilihan komponen faktor adalah seperti yang terdapat pada Rajah 1.

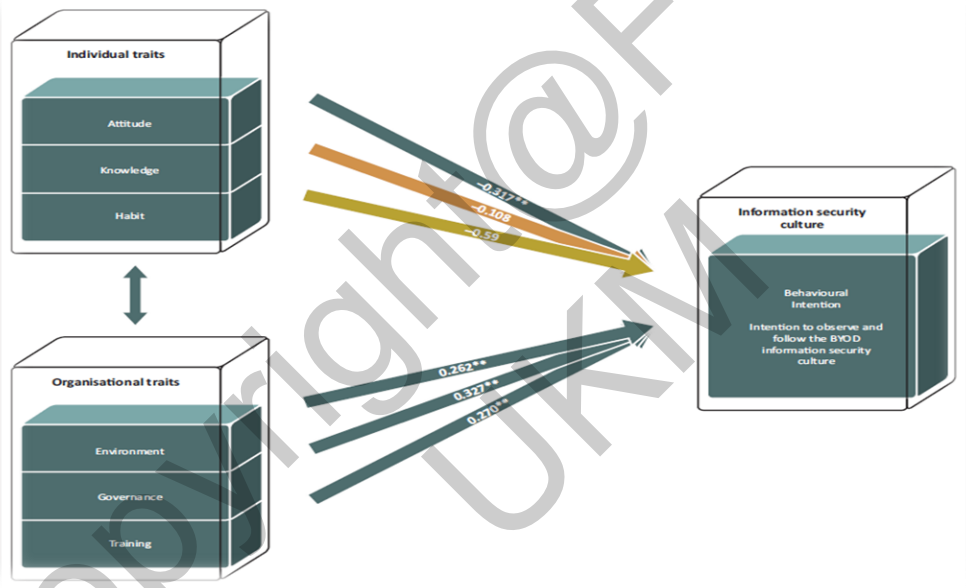


Rajah 1: Pemilihan Komponen Faktor

A. Model *BYOD Information Security Behavioural* (BISB)

Rajah 2 menggambarkan gabungan sifat individu dan organisasi. Dalam model ini, sifat individu dan organisasi saling melengkapi. Ciri-ciri tersebut dikenal pasti dari kajian literatur dan kemudian dirumuskan menjadi sifat niat tingkah laku yang mewakili model *Bring Your Own Device Information Security Behavioural* (BISB) [17].

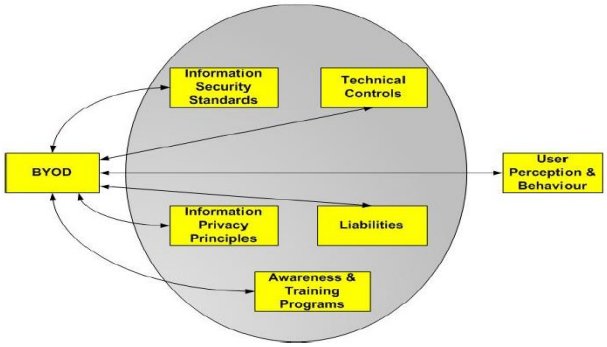
Model BISB yang dirancang untuk memastikan komponen yang diperlukan dibentuk untuk membina pendekatan tingkah laku dalam mengurus pengguna BYOD yang berperanan sebagai pentadbir bagi BYOD.



Rajah 2: *Bring Your Own Device Information Security Behavioural* (BISB) [17].

B. Model *BYOD Policy Management*

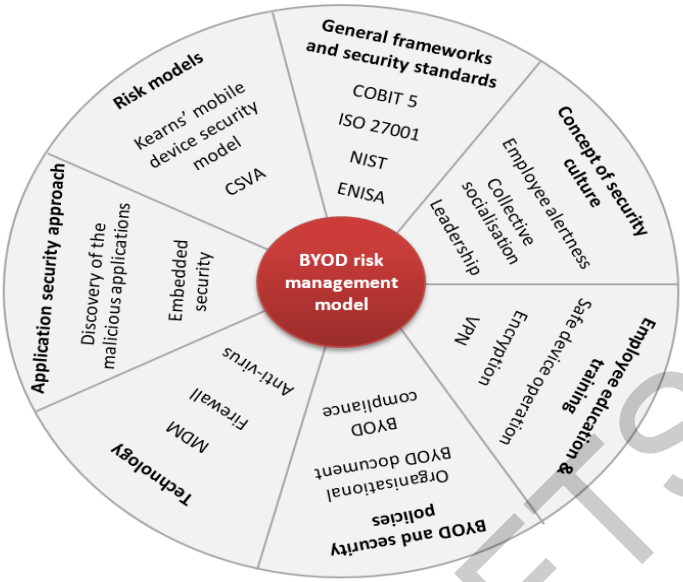
Model *BYOD Policy Based Management* menggambarkan model pengurusan berasaskan polisi BYOD, yang mengkaji setiap komponen untuk mengenal pasti langkah kawalan yang sesuai yang boleh dimasukkan dalam polisi BYOD. Analisis silang mengenai hubungan antara komponen dilakukan untuk mencapai keseimbangan antara keselamatan, privasi dan kerahsiaan, sehingga mengenal pasti langkah-langkah kawalan yang tidak akan mempengaruhi BYOD, organisasi dan pekerja [2]. Model ini ditunjukkan seperti di dalam Rajah 3.



Rajah 3: Model BYOD *Policy-Based Management* [2].

C. Model *BYOD Risk Management*

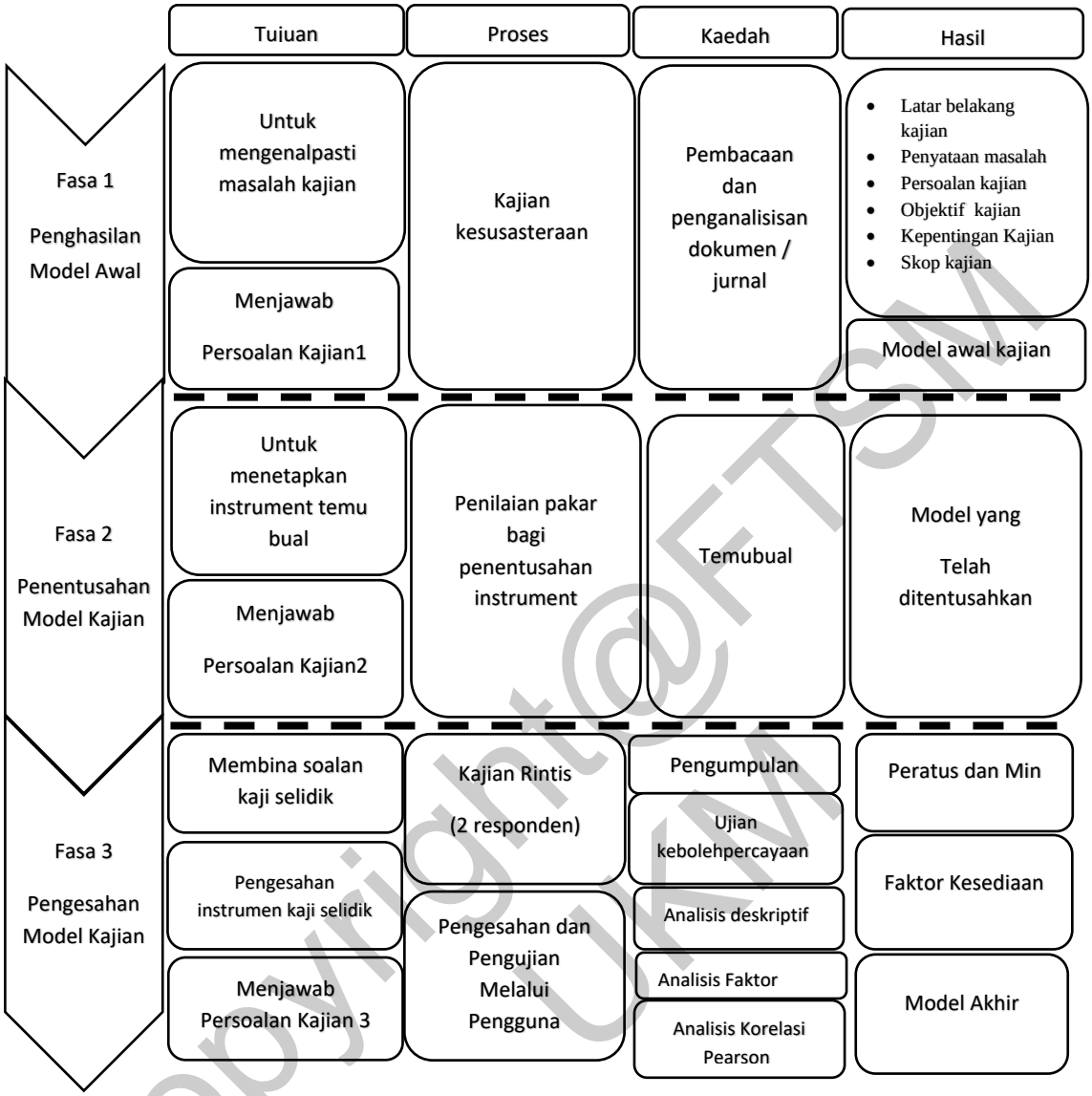
Model pengurusan risiko BYOD yang dicadangkan menunjukkan bahawa menangani risiko yang dikenal pasti harus merangkumi sejumlah pertimbangan. Kerangka keselamatan umum (misalnya COBIT 5, NIST, ENISA) atau piawaian (misalnya siri ISO 27000) harus dipertimbangkan dalam pembakaran terhadap pendekatan organisasi terhadap IT dan keseluruhan pengurusan risiko, yang merangkumi model keselamatan BYOD tertentu [17] atau [19]. Menurut [20] keselamatan teknologi yang disesuaikan dengan model yang diusulkan, harus ditangani dengan memperkenalkan teknologi MDM (*Mobile Devive Technology*), perisian antivirus dan firewall dalam mengenalpasti aplikasi berbahaya atau *malware* yang disertakan dalam aplikasi yang sah. Dasar keselamatan siber organisasi, merangkumi perkara yang berkaitan dengan BYOD dan kepatuhan keselamatan sangat diperlukan untuk menangani risiko yang dikenal pasti oleh kajian ini. Di samping itu, banyak kajian menunjukkan bahawa pekerja selalunya merupakan hubungan keselamatan siber yang paling lemah, oleh itu, pendidikan dan latihan pekerja harus menjadi bahagian utama untuk berjaya menangani risiko BYOD.



Rajah 4: BYOD *Risk Management Model* [20].

3. PENDEKATAN KAJIAN

Kajian melibatkan tiga (3) fasa iaitu (i) fasa penghasilan model awal; (ii) fasa penentusahan model kajian; dan (iii) fasa pengesahan model kajian. Perincian setiap fasa dibahagikan kepada penjelasan terhadap tujuan pelaksanaan, proses dan kaedah yang digunakan serta hasil akhir bagi setiap proses. Gambaran keseluruhan fasa pendekatan kajian adalah seperti di Rajah 5.



Rajah 5: Pendekatan Kajian

3.1 FASA 1: PENGHASILAN MODEL AWAL

A. Mengenalpasti Masalah Kajian

Proses mengenalpasti masalah kajian dilakukan menerusi kajian kesusasteraan untuk mendapatkan maklumat tentang kajian ini. Proses mendapatkan maklumat tertumpu pada pembacaan dan rujukan daripada jurnal, buku, tesis, artikel, garis panduan dan laman web yang berkaitan dengan tahap kesedaran pekerja terhadap penggunaan BYOD.

JADUAL 1: MENGENAL PASTI MASALAH KAJIAN

Proses	Kaedah	Hasil
Kajian Kesusasteraan	• Pembacaan dan penganalisisan terhadap kajian kesusasteraan • Jurnal, artikel, tesis, buku dan Garis Panduan	• Pendahuluan • Penyataan Masalah • Persoalan Kajian • Matlamat dan Objektif Kajian • Kepentingan Kajian • Skop Kajian

Jadual 1 menunjukkan beberapa komponen penting yang telah dikenal pasti melalui kajian kesusasteraan yang dijalankan dan penemuan jurang seterusnya melahirkan isu dan persoalan kajian. Penerangan secara terperinci berkenaan pendahuluan, penyataan masalah, persoalan kajian, matlamat, objektif kajian, kepentingan kajian serta skop kajian telah diterangkan sebelum ini.

B. Merangka Model Awal

Dalam merangka penghasilan model awal, kajian kesusasteraan telah dilakukan meliputi aktiviti pembacaan jurnal, buku dan artikel yang berkaitan dalam bidang BYOD. Kajian kesusasteraan mampu meningkatkan pemahaman terhadap bidang kajian dan segala aspek yang berkaitan dengan kajian dapat diterokai. Melalui melalui kajian kesusasteraan juga, ianya membantu dalam memahami dan mengenal pasti jurang pengetahuan yang wujud hasil daripada kajian lampau penyelidik dalam bidang yang hendak dikaji dan juga dokumen DKICT sedia ada yang merupakan panduan kerajaan dalam mematuhi pelaksanaan penggunaan BYOD di kalangan penjawat awam.

JADUAL 2: MERANGKA MODEL AWAL KAJIAN

Proses	Kaedah	Hasil
Merangka model awal	• Pembacaan dan penganalisisan terhadap kajian kesusasteraan berkenaan tahap kesedaran pekerja terhadap penggunaan BYOD • Jurnal, artikel, tesis dan garis panduan DKICT	• Model awal kajian

Jadual 2 menerangkan proses yang terlibat dalam merangka model awal kajian. Dalam menghasilkan model awal kajian, aspek kesedaran dan faktor-faktor dikenal pasti melalui kajian kesusasteraan dan kajian lampau. Pembacaan jurnal dan artikel lepas dan seterusnya membentuk

Model awal kajian. Penghuraian secara terperinci model awal kajian diterangkan pada Bab II. Proses kajian kesusasteraan menggunakan teknik carian melalui *Google Scholar* dan *Scopus.* Hasil carian menemui beberapa aspek dan faktor dalam menentukan tahap kesedaran pekerja terhadap penggunaan BYOD.

3.2 FASA 2: PENENTUSAHAN MODEL KAJIAN

Kajian ini menggunakan pendekatan kaedah kajian campuran yang bersifat kuantitatif dan kualitatif. Menurut [21], pendekatan kuantitatif ialah satu usaha membentuk prinsip dan peraturan yang mengandaikan realiti sosial sebagai objektif dan terpisah atau tidak, berkaitan dengan individu. Sementara itu, pendekatan kualitatif pula menekankan kepentingan pengalaman subjektif individu yang perlu dianalisis secara kualitatif dan realiti sosial mempunyai makna tertentu yang bersifat subjektif dan personal. Bagi tujuan pengumpulan data, pendekatan kuantitatif yang digunakan iaitu instrumen soal selidik dan pendekatan kualitatif iaitu instrumen temu bual.

3.3 FASA 3: PENGESAHAN MODEL KAJIAN

Fasa ketiga adalah proses pengesahan instrumen kaji selidik terhadap penghasilan borang soal selidik yang dilakukan hasil daripada temu bual dengan pihak pakar pada fasa kedua. Penilaian pakar bagi kesahan kandungan (*content validity*) bertujuan untuk memastikan instrumen kajian kerangka kerja dibangunkan menggunakan bahasa yang sesuai dan mudah difahami di samping memastikan setiap item yang dihasilkan berkualiti.

3.4 ANALISIS DATA

A. Ujian Kebolehpercayaan

Ujian kebolehpercayaan bermaksud kebolehan sesuatu alat ukur atau instrumen kajian menghasilkan keputusan yang tekal atau konsisten setiap kali pengukuran sesuatu konsep dan aspek dilakukan. Analisis ujian kebolehpercayaan dilakukan ke atas instrumen soalan kaji selidik dengan menggunakan perisian SPSS. Menurut [22], nilai *Cronbach's Alpha (*CA) boleh mengukur

tahap kebolehpercayaan item untuk menguji kesahihan soalan kaji selidik yang dibangunkan. Nilai julat kebolehpercayaan (CA) adalah di antara 0 dan 1 [23], Menurut [24], panduan nilai kebolehpercayaan (CA) adalah seperti di Jadual 3.

JADUAL 3 : PANDUAN TAHAP NILAI PEKALI KEBOLEHPERCAYAAN [24]

Nilai *alpha* (α)	**Tahap Kebolehpercayaan**
0.90 atau lebih	Cemerlang
0.80 – 0.89	Baik
0.70 – 0.79	Diterima
0.60 – 0.69	Diragui
0.50 – 0.59	Lemah
Kurang dari 0.50	Ditolak

B. Ujian Skor Min

Dalam kajian ini, tahap kesedaran pekerja terhadap BYOD dinilai berdasarkan analisis skor min mengikut faktor-faktor yang dikenal pasti pada model awal dan di ukur dengan menggunakan skala likert 7 mata. Nilai-nilai ini kemudiannya di kategori kepada tiga (3) iaitu rendah, sederhana dan tinggi untuk menentukan tahap kesedaran pekerja terhadap BYOD. Skor min yang di tafsir sebagaimana yang dicadangkan oleh [25], merujuk kepada jadual 4. Sekiranya item yang di analisis berada pada julat 1.00-3.26, ini menunjukkan tahap kesedaran pekerja terhadap membawa peranti BYOD berada pada tahap yang rendah. Keputusan sederhana pula merangkumi skor min antara 3.27-5.14. Manakala skor min 5.15-7.00 pula menunjukkan tahap kesedaran pekerja yang tinggi terhadap BYOD.

JADUAL 4: TAFSIRAN DAN TAHAP KECENDERUNGAN MIN [25]

Skor Min	**Tahap Kecenderungan**
1.00 – 3.26	Rendah
3.27 – 5.14	Sederhana
5.15 – 7.00	Tinggi

C. Analisis Faktor

Analisis faktor adalah sebuah teknik yang digunakan untuk mencari faktor-faktor yang mampu menjelaskan hubungan atau korelasi antara berbagai indikator independen yang

diobservasi. Menurut [26], analisis faktor adalah alat analisis statistik yang digunakan untuk mengurangkan faktor-faktor yang mempengaruhi pemboleh ubah kepada beberapa set indikator, tanpa kehilangan maklumat yang signifikan.

Secara umum, proses analisis faktor ialah memilih pemboleh ubah yang patut dimasukkan dalam analisis faktor. Oleh kerana analisis faktor mengumpulkan nombor pemboleh ubah, maka ianya perlu menjadi korelasi (hubungan) yang cukup kuat di antara pemboleh ubah, sehingga pengelompokan berlaku. Setelah sejumlah pemboleh ubah dipilih, ianya digabungkan menjadi satu atau beberapa kumpulan pemboleh ubah. Kaedah yang sering digunakan bagi analisis faktor adalah *Principal Component Analysis* dan *Maximum Likehood.*

4. HASIL PENGUJIAN

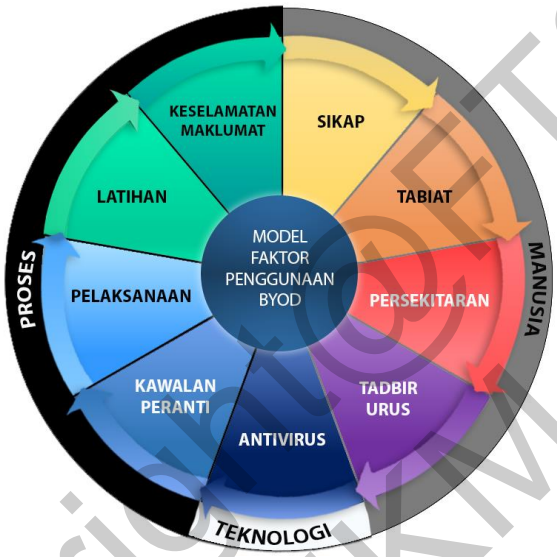
Kajian sebenar telah dilakukan pada 16 – 31 Mac 2020 iaitu selama 15 hari di Unit Penyelarasan dan Pelaksanaan, Jabatan Perdana Menteri (ICU JPM). Borang soal selidik telah dihantar menggunakan e-mel pejabat dan daripada 70 orang responden yang dihantar, sebanyak 53 responden telah memberikan maklum balas. Borang soal selidik di hantar secara atas talian menggunakan platform *Google Forms.* Seramai 70 orang responden telah di pilih untuk menjawab soalan soal selidik ini yang terdiri daripada kategori pengurusan atasan, pengurusan dan profesional dan kumpulan pelaksana. Ringkasan maklumat pengumpulan data adalah seperti di Jadual 5.

JADUAL 5: MAKLUMAT PENGUMPULAN

Tarikh	16 – 31 Mac 2020 (15 hari)
Tajuk	Model Tahap Kesedaran Pekerja Terhadap Penggunaan BYOD di Sektor Awam
Entiti terlibat	Unit Penyelarasan dan Pelaksanaan Jabatan Perdana Menteri
Kumpulan sasaran	• Kumpulan Pengurusan dan Professional • Kumpulan Sokongan I (Gred 17 – 40) • Kumpulan Sokongan II (Gred 1 – 16)
Bilangan responden	• 53 daripada 70 responden
Kaedah agihan	• Secara atas talian menggunakan google *form survey*

4.1 PENGESAHAN MODEL

Pengesahan model daripada pakar berlandaskan tiga (3) Faktor Utama iaitu (i) manusia; (ii) proses; dan (iii) teknologi. Oleh yang demikian, pakar menyarankan bagi Faktor Manusia merangkumi komponen tingkah laku manusia. Bagi Faktor Proses ianya terbahagi kepada komponen faktor pengetahuan dan faktor polisi, manakala bagi Faktor Teknologi diwujudkan, dan komponen faktornya adalah antivirus seperti di Rajah 6.



Rajah 6: Model Kajian Selepas Ditentusahan oleh Pakar

4.2 UJIAN KEBOLEHPERCAYAAN

Instrumen kaji selidik kajian ini mengandungi empat (4) bahagian. Ujian kebolehpercayaan dilakukan pada setiap bahagian dan keputusan ujian adalah seperti Jadual 6:

JADUAL 6: KEPUTUSAN UJIAN *CRONBACH'S ALPHA* (CA) PADA INSTRUMEN KAJIAN

Kategori	***Cronbach's Alpha***	**No Item**
M (Faktor Manusia)	0.896	9
K (Faktor Pengetahuan)	0.803	6
P (Faktor Polisi)	0.883	8
T (Faktor Teknologi)	0.944	4

Daripada hasil analisis kebolehpercayaan pada kategori faktor manusia adalah 0.896 (baik), faktor proses (pengetahuan) adalah 0.803 (baik), faktor proses (polisi) adalah 0.883 (baik) dan faktor teknologi adalah 0.944 (cemerlang). Ini menunjukkan setiap item tersebut adalah seragam dan mempunyai hubung kait antara satu sama lain pada setiap kategori. Selain itu juga, purata keseluruhan instrumen kajian juga diuji kebolehpercayaan faktor modul dan didapati hasil analisis adalah 0.962 (cemerlang). Ini menunjukkan instrumen kaji selidik yang terdiri daripada 27 item adalah konsisten dan mempunyai hubung kait antara satu sama lain.

4.3 UJIAN SKOR MIN

Secara keseluruhannya, skor min bagi keseluruhan kaji selidik adalah di antara 5.45 – 6.43 seperti pada Jadual 7. Berdasarkan tafsiran skor min yang ditetapkan oleh [27] nilai-nilai tersebut menunjukkan tahap yang tinggi. Skor ini juga menunjukkan bahawa tahap kesedaran pekerja terhadap penggunaan BYOD berada di tahap yang tinggi.

JADUAL 7: SKOR MIN DAN TAHAP KESEDARAN RESPONDEN

Kod Item	Soalan	Min	Tahap Kesedaran
M1	Anda menetapkan kata laluan (screen lock) pada peranti mudah alih anda.	6.43	Tinggi
M2	Anda menghantar e-mel/ memuat turun dokumen pejabat menggunakan sambungan WiFi yang selamat (Secured WiFi).	5.79	Tinggi
M3	Anda menglog keluar daripada sebarang aplikasi selepas menggunakan aplikasi tersebut.	6.00	Tinggi
M4	Anda tidak pernah meninggalkan peranti mudah alih anda tanpa diawasi?	6.11	Tinggi
M5	Anda menggunakan kata laluan yang berbeza pada urusan rasmi seperti e-mel pejabat dengan akaun sosial.	5.92	Tinggi
M6	Anda menyimpan maklumat mesyuarat di dalam kalendar peranti peribadi anda.	5.68	Tinggi
M7	Anda membuat laporan serta mengambil tindakan sewajarnya jika peranti mudah alih anda hilang?	5.66	Tinggi
M8	Penggunaan peranti mudah alih anda memudahkan anda melakukan tugasan harian aktiviti personal.	6.26	Tinggi
M9	Anda tidak berkongsi menggunakan peranti mudah alih anda dengan ahli keluarga.	5.92	Tinggi
K1	Anda memahami apakah itu ‘Membawa Peranti Anda Sendiri’ (BYOD).	5.49	Tinggi
K2	Pihak pengurusan memberikan penerangan dan pendedahan tentang penggunaan peranti BYOD di pejabat.	5.40	Tinggi
K3	Anda tidak menyimpan sebarang maklumat rasmi dan maklumat terperingkat di peranti BYOD anda.	5.74	Tinggi

bersambung…

…sambungan

K4	Penggunaan peranti BYOD di pejabat meningkatkan risiko kebocoran maklumat dan ancaman keselamatan ICT.	5.53	Tinggi
K5	Memuat turun atau memasang sebarang aplikasi percuma boleh mendedahkan maklumat peribadi anda kepada pihak ketiga.	5.89	Tinggi
K6	Penggunaan WIFI Awam (Open WiFi) boleh mengundang kebocoran maklumat atau data di dalam peranti mudah alih anda.	5.70	Tinggi
P1	Adakah anda setuju dengan Polisi BYOD di dalam Dasar Keselamatan ICT?	5.55	Tinggi
P2	Adakah anda menyokong pelaksanaan Polisi BYOD di Jabatan / Kementerian anda?	5.74	Tinggi
P3	Pengguna BYOD bertanggungjawab dalam mematuhi tatacara penggunaan dan pengurusan peranti BYOD.	5.57	Tinggi
P4	Anda mendaftar peralatan BYOD sebelum menggunakannya di pejabat.	5.68	Tinggi
P5	Pelaksanaan polisi BYOD tidak akan mengganggu sistem pada peranti mudah alih anda.	5.91	Tinggi
P6	Jabatan / Kementerian anda melakukan pemantauan ke atas kegunaan peranti mudah alih anda?	6.23	Tinggi
P7	Anda meletakkan kata laluan atau kod penyulitan pada fail data di peranti BYOD anda untuk tujuan keselamatan.	5.92	Tinggi
P8	Adalah menukarkan kata laluan pada peranti BYOD anda setiap tiga bulan.	6.38	Tinggi
T1	Adakah memasang antivirus pada peranti persendirian anda dapat mengekang kemasukan sebarang virus / malware ke dalam peranti persendirian anda?	5.79	Tinggi
T2	Anda sentiasa melakukan pengemaskinian terhadap patches antivirus terkini pada peranti persendirian anda.	5.57	Tinggi
T3	Anda tahu penggunaan antivirus dapat melindungi peranti persendirian anda daripada ancaman oleh pihak yang tidak bertanggungjawab.	5.45	Tinggi
T4	Teknologi anti-theft dapat melindungi data pada peranti BYOD dan membantu mencari peranti BYOD jika hilang atau dicuri.	5.66	Tinggi

4.4 UJIAN ANALISIS FAKTOR

Ujian analisis faktor kajian ini dijalankan dengan menggunakan analisis komponen prinsipal. Data tersebut kemudiannya diputar dengan mengguna pusingan varimax dan hasilnya adalah seperti di dalam Jadual 8. Hasil pusingan varimax menunjukkan, nilai item menjadi lebih tinggi dan hampir dekat di antara satu sama lain. Ini membukti bahawa hubungan korelasi di antara item dengan faktor yang terbentuk dan ini merupakan kunci untuk memahami sifat faktor-faktor tersebut. Berdasarkan bukti ini, putaran varimax dapat digunakan untuk menghasilkan tafsiran data yang baik.

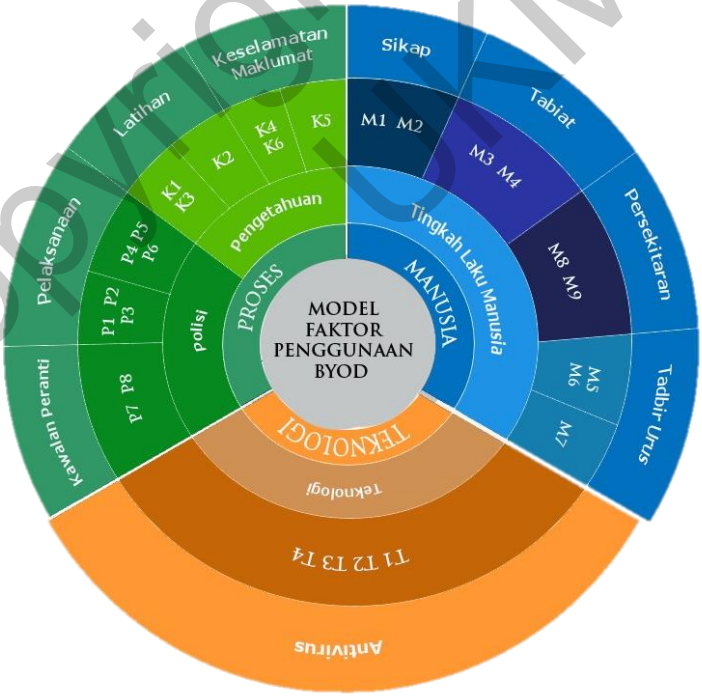
JADUAL 8: MATRIKS KOMPONEN BAGI ANALISIS FAKTOR

Kod Item	Soalan	Komponen	
		1	2
M1	Anda menetapkan kata laluan (screen lock) pada peranti mudah alih anda.	.893	.449
M2	Anda menghantar e-mel/ memuat turun dokumen pejabat menggunakan sambungan WiFi yang selamat (Secured WiFi)	.893	
M3	Anda menglog keluar daripada sebarang aplikasi selepas menggunakan aplikasi tersebut.	.819	
M4	Anda tidak pernah meninggalkan peranti mudah alih anda tanpa diawasi?	.819	.574
M5	Anda menggunakan kata laluan yang berbeza pada urusan rasmi seperti e-mel pejabat dengan akaun sosial.	.922	
M6	Anda menyimpan maklumat mesyuarat di dalam kalendar peranti peribadi anda.	.856	
M7	Anda membuat laporan serta mengambil tindakan sewajarnya jika peranti mudah alih anda hilang?		.952
M8	Penggunaan peranti mudah alih anda memudahkan anda melakukan tugasan harian aktiviti personal.	.797	
M9	Anda tidak berkongsi menggunakan peranti mudah alih anda dengan ahli keluarga.	.797	.604
K1	Anda memahami apakah itu ‘Membawa Peranti Anda Sendiri’ (BYOD).	.830	
K2	Pihak pengurusan memberikan penerangan dan pendedahan tentang penggunaan peranti BYOD di pejabat.		.982
K3	Anda tidak menyimpan sebarang maklumat rasmi dan maklumat terperingkat di peranti BYOD anda.	.845	
K4	Penggunaan peranti BYOD di pejabat meningkatkan risiko kebocoran maklumat dan ancaman keselamatan ICT.	.938	
K5	Memuat turun atau memasang sebarang aplikasi percuma boleh mendedahkan maklumat peribadi anda kepada pihak ketiga.		.945
K6	Penggunaan WIFI Awam (Open WiFi) boleh mengundang kebocoran maklumat atau data di dalam peranti mudah alih anda.	.932	
P1	Adakah anda setuju dengan Polisi BYOD di dalam Dasar Keselamatan ICT?	.828	
P2	Adakah anda menyokong pelaksanaan Polisi BYOD di Jabatan / Kementerian anda?	.893	
P3	Pengguna BYOD bertanggungjawab dalam mematuhi tatacara penggunaan dan pengurusan peranti BYOD.	.895	
P4	Anda mendaftar peralatan BYOD sebelum menggunakannya di pejabat.	.669	.686
P5	Pelaksanaan polisi BYOD tidak akan mengganggu sistem pada peranti mudah alih anda.	.776	.798
P6	Jabatan / Kementerian anda melakukan pemantauan ke atas kegunaan peranti mudah alih anda?		.861
P7	Anda meletakkan kata laluan atau kod penyulitan pada fail data di peranti BYOD anda untuk tujuan keselamatan.	.890	.455
P8	Adalah menukarkan kata laluan pada peranti BYOD anda setiap tiga bulan.	.890	
T1	Adakah memasang antivirus pada peranti persendirian anda dapat mengekang kemasukan sebarang virus / malware ke dalam peranti persendirian anda?	.910	
T2	Anda sentiasa melakukan pengemaskinian terhadap patches antivirus terkini pada peranti persendirian anda.	.935	
T3	Anda tahu penggunaan antivirus dapat melindungi peranti persendirian anda daripada ancaman oleh pihak yang tidak bertanggungjawab.	.902	
T4	Teknologi anti-theft dapat melindungi data pada peranti BYOD dan membantu mencari peranti BYOD jika hilang atau dicuri.	.960	

Kaedah pengekstrakan: Analisis komponen prinsipal

4.5 MODEL AKHIR KAJIAN

Berdasarkan penentusahan dan pengesahan yang dibuat oleh pakar, model akhir kajian adalah seperti di Rajah 7. Daripada hasil, setiap komponen dibahagikan kepada dua (2) kategori iaitu formaliti dan simpanan. Bagi faktor Manusia untuk komponen sikap, M1 dan M2 diletakkan pada kategori formaliti. Manakala untuk komponen tabiat, M3 dan M4 diletakkan pada kategori formaliti. Untuk komponen tadbir urus M5 dan M6 diletakkan pada kategori formaliti, dan M7 adalah simpanan dan bagi komponen persekitaran, M8 dan M9 diletakkan pada kategori formaliti. Bagi faktor Pengetahuan untuk komponen latihan, K1 dan K3 diletakkan pada kategori formaliti dan K2 pada simpanan. Manakala untuk komponen keselamatan maklumat, item K4 dan K6 diletakkan pada kategori formaliti dan item K5 pada simpanan. Bagi faktor polisi pula, komponen pelaksanaan, P1, P2 dan P3 diletakkan pada kategori formaliti, manakala item P4, P5 dan P6 diletakkan pada kategori simpanan. Bagi komponen kawalan peranti item P7 dan P8 diletakkan pada kategori formaliti. Dan bagi faktor Teknologi, keseluruhan komponen antivirus T1, T2, T3 dan T4 berada di dalam kategori yang sama. Jadual 9 menunjukkan keseluruhan komponen model akhir yang dipecahkan mengikut kategori.



Rajah 7: Model Akhir Kajian

JADUAL 9: KOMPONEN MODEL AKHIR MENGIKUT KATEGORI

MANUSIA	Tingkah Laku Manusia	Sikap	M1	Anda menetapkan kata laluan (screen lock) pada peranti mudah alih anda
			M2	Anda menghantar e-mel/ memuat turun dokumen pejabat menggunakan sambungan WiFi yang selamat (Secured WiFi)
		Tabiat	M3	Anda menglog keluar daripada sebarang aplikasi selepas menggunakan aplikasi tersebut.
			M4	Anda tidak pernah meninggalkan peranti mudah alih anda tanpa diawasi.
		Tadbir Urus	M5	Anda menggunakan kata laluan yang berbeza pada urusan rasmi seperti e-mel pejabat dengan akaun sosial
			M6	Anda menyimpan maklumat mesyuarat di dalam kalendar peranti peribadi anda.
			M7	Anda membuat laporan serta mengambil tindakan sewajarnya jika mendapati peranti mudah alih anda hilang.
		Persekitaran	M8	Penggunaan peranti mudah alih anda memudahkan anda melakukan tugasan harian serta melakukan aktiviti personal.
			M9	Anda tidak berkongsi menggunakan peranti mudah alih anda dengan ahli keluarga.
PROSES	Pengetahuan	Latihan	K1	Adakah anda memahami apakah itu 'Membawa Peranti Anda Sendiri' (BYOD)
			K2	Pihak pengurusan memberikan penerangan dan pendedahan tentang penguna peranti BYOD di pejabat
			K3	Anda tidak menyimpan sebarang maklumat rasmi dan maklumat terperingkat di peranti BYOD anda
		Keselamatan Maklumat	K4	Penggunaan peranti BYOD di pejabat meningkatkan risiko kebocoran maklumat dan ancaman keselamatan ICT
			K5	Memuat turun atau memasang sebarang aplikasi percuma boleh mendedahkan maklumat peribadi anda kepada pihak ketiga
			K6	Penggunaan WIFI Awam (Open WiFi) boleh mengundang kebocoran maklumat atau data di dalam peranti mudah alih anda
	Polisi	Pelaksanaan	P1	Adakah anda setuju dengan Polisi BYOD di dalam Dasar Keselamatan ICT?
			P2	Adakah anda menyokong pelaksanaan Polisi BYOD di Jabatan / Kementerian anda?
			P3	Pengguna BYOD bertanggungjawab dalam mematuhi tatacara penggunaan dan pengurusan peranti BYOD.
			P4	Anda mendaftar peralatan BYOD sebelum menggunakannya di pejabat
			P5	Pelaksanaan polisi BYOD tidak akan mengganggu sistem peranti mudah alih anda.
			P6	Jabatan / Kementerian anda melakukan pemantauan ke atas kegunaan peranti mudah alih anda?
		Kawalan Peranti	P7	Anda meletakkan kata laluan atau kod penyulitan pada fail data di peranti BYOD anda untuk tujuan keselamatan.
			P8	Adalah menukarkan kata laluan pada peranti BYOD anda setiap tiga bulan
TEKNOLOGI	Teknologi	Antivirus	T1	Adakah memasang antivirus pada peranti persendirian anda dapat mengekang kemasukan sebarang virus / malware ke dalam peranti persendirian anda?
			T2	Anda sentiasa melakukan pengemaskinian terhadap patches antivirus terkini pada peranti persendirian anda?
			T3	Anda tahu penggunaan antivirus dapat melindungi peranti persendirian anda daripada ancaman oleh pihak yang tidak bertanggungjawab.
			T4	Teknologi anti-theft dapat melindungi data pada peranti BYOD dan membantu menmcari peranti BYOD jika hilang atau dicuri.

5. KESIMPULAN

5.1 PENCAPAIAN OBJEKTIF

Secara keseluruhan, kajian ini berjaya memenuhi tiga (3) objektif kajian yang telah dinyatakan di dalam Bab satu. Berikut adalah rumusan penemuan kajian terhadap persoalan kajian.

A. Mengenal Pasti Faktor Tahap Kesedaran Pekerja Terhadap Penggunaan BYOD Di Sektor Awam

Objektif pertama adalah untuk mengenal pasti faktor tahap kesedaran pekerja terhadap penggunaan BYOD di sektor awam. Pembangunan model awal kajian ini adalah bermula dengan melakukan kajian kesusasteraan dan kajian ke atas jurnal-jurnal yang lepas mengenai BYOD berdasarkan persoalan kajian dan objektif kajian yang hendak dicapai. Model awal kajian ini terdiri

daripada tiga (3) komponen faktor utama, iaitu tingkah laku manusia, pengetahuan dan polisi. Berdasarkan komponen faktor utama ditemukan lapan (8) elemen faktor yang dikenalpasti mempengaruhi tahap kesedaran pekerja terhadap penggunaan BYOD iaitu sikap, tabiat, persekitaran, tadbir urus, keselamatan maklumat, latihan, pelaksanaan dan kawalan peranti.

B. Membangunkan Model Tahap Kesedaran Pekerja Terhadap Penggunaan BYOD Di Sektor Awam

Objektif kedua adalah membangunkan model tahap kesedaran pekerja terhadap penggunaan BYOD di Sektor Awam berdasarkan kajian lampau penyelidik dalam bidang yang dikaji dan juga dokumen DKICT sedia ada yang merupakan panduan kerajaan dalam mematuhi pelaksanaan penggunaan BYOD di kalangan penjawat awam. Pembangunan model dalam kajian ini adalah bermula dengan melakukan kajian kesusasteraan terhadap model faktor yang mempengaruhi penggunaan BYOD dari aspek tingkah laku manusia, polisi dan pengetahuan tentang BYOD. Seterusnya, model awal kajian ini diteliti dan disahkan oleh dua (2) orang pakar yang berpengalaman dalam bidang dasar dan keselamatan ICT. Hasil temu bual bersama pakar telah membuahkan cadangan serta idea pakar, lalu diteliti dan dianalisa bagi menghasilkan model yang ditentusahan oleh pakar.

C. Mengesahkan keberkesanan model dengan menggunakan kajian kes yang dipilih terhadap model yang dibangunkan.

Objektif ketiga adalah mengesahkan keberkesanan model dengan menggunakan kajian kes yang dipilih terhadap model yang telah dibangunkan dan ditentusahan. Di dalam fasa tiga (3) pengesahan model kajian melibatkan pengujian model akhir dan soal selidik. Proses penilaian dilakukan menggunakan borang soal selidik secara atas talian menggunakan Google Form. Hasil analisis mendapati secara keseluruhan responden bersetuju dan menerima model yang dicadangkan dan sememangnya terbukti mencakupi kesemua aspek yang dibincangkan jika dilihat dari hasil analisis deskriptif dan analisis faktor serta model akhir yang dikemukakan. Oleh itu aspek faktor manusia, proses dan teknologi perlu diberi perhatian lebih serius dalam memupuk tahap kesedaran di sesebuah agensi.

5.2 SUMBANGAN KAJIAN

Berdasarkan kajian yang telah dijalankan, terdapat empat (4) sumbangan utama yang telah diberikan dalam kajian ini. Sumbangan-sumbangan tersebut ialah:

a) Mengenalpasti aspek faktor kelemahan dan pengukuhan keselamatan data perlu di patuhi sebelum pelaksanaan polisi BYOD di sesebuah agensi.

b) Menghasilkan model baru dengan menggabungkan 3 kajian yang telah dilakukan bersama input dari pihak pakar. Model baru yang dihasilkan boleh digunakan untuk mengukur tahap kesedaran pengguna terhadap penggunaan BYOD.

c) Sebagai garis panduan dan rujukan kepada sektor awam Malaysia terhadap penggunaan peranti BYOD di agensi masing-masing. Juga model yang dibangunkan boleh diguna pakai dan diperluaskan ke sektor swasta dalam membantu memperkukuhkan aspek keselamatan data dan maklumat di organisasi swasta.

d) Mempertingkatkan tahap kesedaran penjawat awam tentang penggunaan BYOD dan tahap kesediaan organisasi terhadap keselamatan data dan pengenalpastian jurang yang harus ditambah baik.

5.3 CADANGAN KAJIAN MASA DEPAN

Kajian ini berjaya menghasilkan satu model untuk menentukan tahap penilaian organisasi rumusan hasil penemuan kajian yang pertama adalah bagi mencapai objektif kajian dan seterusnya menjawab persoalan kajian yang telah dinyatakan di dalam bab pertama. Kajian lanjutan adalah dicadangkan untuk penyelidikan masa depan. Berikut adalah beberapa cadangan perluasan kerja dan cadangan kajian masa depan:

a) Memperluaskan instrumen kajian dengan mengadakan proses temu bual bersama beberapa pakar iaitu lebih dari dua (2) orang. Pemilihan pakar hendaklah melibatkan sektor awam dan sektor swasta bagi mendapatkan pendekatan yang berbeza di dalam bidang kerja yang berlainan serta melakukan pemerhatian ke atas aktiviti penggunaan peranti BYOD.

b) Kajian boleh diperluaskan ke agensi-agensi Sektor Awam yang lain. Maklumat tersebut boleh dibandingkan untuk melihat kesesuaian dan keberkesanan model yang digunakan. Penambahan saiz sampel dan skop kajian yang luas supaya hasil dapatan kajian lebih bermakna dan lebih mudah diterima oleh pelbagai pihak sebagai rujukan.

c) Mendalami serta melakukan kajian yang lebih menyeluruh terhadap faktor teknologi di mana melalui faktor teknologi, aspek keselamatan maklumat, peranti dan data dapat diperkukuhkan dengan penggunaan pengurusan peranti mudah alih (MDM). Fungsi MDM boleh mengehadkan ciri aplikasi tertentu pada peranti BYOD yang berdaftar dengan MDM.

RUJUKAN

[1] Marziana Abdul Majid, Zulkefli Mansor, Rossilawati Sulaiman & Asrina Suriani Mohd Yunus (2018). Pemerhatian Awalan ke atas Amalan Membawa Peralatan Sendiri (BYOD) dalam Organisasi ms 1–7.

[2] Garba, A. B, Armarego, J., Murray, D. & April, M. 2015. *A Policy-Based Framework for Managing BYOD Environments - International Journal of Emerging Trends & Technology in Computer Science* (IJETTCS), Vol. 4: p 189-198.

[3] Pinchot, J. 2016. *Bring Your Own Device To Work: Benefits, Security risks and Governance Issues* 16(Iii): 238–244.

[4] Dhingra, M. 2015. *Legal Issues in Secure Implementation of Bring Your Own Device. Procedia - Procedia Computer Science 78*(December 2015): 179–184. doi:10.1016/j.procs.2016.02.030.

[5] Fatimah Alzair. 2016. *A critical review of the governance of personal IT devices in work environments. A dissertation for degree of Master of Business, Aukland University of Technology.*

[6] Miller, K.W., Voas, J. and Hurlburt, G.F.; *"BYOD: Security and Privacy Consideration" IT Professional, Volume 14, Issue*: 5, 2012 , Page(s): 53 – 55.

[7] Georgiadis, C., Stiakakis, E. & Andronoudi, A. 2014. *The Significance of Mobile Security Breaches in Terms of Their Economic Impact on Users. International Conference on Mobile Business* 2014.

[8] Pillay, A., Nham, E., Tan, G. & Diaki, H. 2013. *Does BYOD increase risks or drive benefits*? Dtl.Unimelb.Edu.Au (2013): 1–8. Retrieved from https://minerva-access.unimelb.edu.au/bitstream/handle/11343/33345/300314_2013_Tan_Risk.pdf?sequence=1%0Ahttps://minerva-access.unimelb.edu.au/handle/11343/33345.

[9] ICU JPM, Unit Penyelarasan dan Pelaksanaan, Jabatan Perdana Menteri. Dasar Keselamatan ICT (DKICT) ICU JPM Versi 5.3 – (2016).

[10] Mohd Yusri Jusoh, Haryani Haron & Jasber Kaur (2017). *A Conceptual Framework for BYOD to Support Green Computing in Public Sector. International Journal of Control Theory and Applications* 10(07): 27–34.

[11] Willis, D. A. 2013. *Bring Your Own Device: The Facts and the Future. Gartner Inc.*

[12] Györy, Jo, A., Cleven, A., Uebernickel, F. & Brenner, W. 2012. Exploring *The Shadows: IT Governance Approaches to User-Driven Innovation. ECIS 2012 Proceedings.shi, A., Kale, S., Chandel, S. & Pal, D. 2015. Likert Scale: Explored and Explained. British Journal of Applied Science & Technology* 7(4): 396–403. doi:10.9734/bjast/2015/14975.

[13] Harris, J.,Ives, B. & Junglas, I. 2012. *IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. MIS Quarterly Executive*, 11.

[14] Nicol, D. 2013. *Mobile Strategy: How Your Company Can Win by Embracing Mobile Technologies, New Jersey, Pearson Education.*

[15] Van Heck, E., Van Baalen, P., Van Der Meulen, N. & Van Oosterhout, M. 2012. *Achieving High Performance in a Mobile and Green Workplace: Lessons from Microsoft Netherlands. MIS Quarterly Executive*, 11, 175-188.

[16] Farrel, D. 2014. *The Factors That Influence the Implementation of A BYOD Program. Masters Thesis*, September 2014.

[17] Musarurwa, Alfred., Flowerday, Stephen.,Cilliers, L. 2018. *Students' perceptions of the infopreneurship education in the Department of Records and Archives Management at the National University of Science and Technology. SA Journal of Information Management* 18(1): 1–9. doi:10.4102/sajim.v18i1.717.

[18] Almarhabi, K., Jambi, K., Eassa, F. & Batarfi, O. 2018. *A Proposed Framework for Access Control in the Cloud and BYOD Environment 18(2): - IJCSNS International Journal of Computer Science and Network Security,* VOL.18 No.2, February 2018, pp. 144–152.

[19] Almarhabi, K., Jambi, K., Eassa, F. & Batarfi, O. 2018. *A Proposed Framework for Access Control in the Cloud and BYOD Environment 18(2): - IJCSNS International Journal of Computer Science and Network Security,* VOL.18 No.2, February 2018, pp. 144–152.

[20] Veljkovic, I. & Budree, A. 2019. *Development of Bring-Your-Own-Device Risk Management Model : A Case Study From a South African Organisation* 22(2015): 1–14.

[21] Neuman, W. L. (2000). *Social research methods: Qualitative and Quantative Approaches.* 3rd Edition, Boston, MA: Allyn and Bacon.

[22] Taber, K. S. 2018. *The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. Research in Science Education* 48(6): 1273–1296. doi:10.1007/s11165-016-9602-2.

[23] Gliem, J.A., & Gliem, R.R. (2003). *Calculating, interpreting, and reporting Cronbach's Alpha reliability coefficient for likert-type scales. Paper presented at the 2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education*.

[24] George, D., & Mallery, P. (2003). SPSS *for Windows step by step: a simple guide and reference* (4th edn.). Boston: Allyn & Bacon.

[25] Landell, K. (1997). *Management by menu*. London: Wiley and Sons Inc.

[26] Kass, A. Richard & Howard E.A. Tinsley (2018). *Factor Analysis. Journal of Leisure Research. Volume* 11, 1979 - Issue 2. doi.org/10.1080/00222216.1979.11969385.

[27] Landell, K. (1997). *Management by menu*. London: Wiley and Sons Inc.