MODEL TAHAP KESEDARAN KESELAMATAN MAKLUMAT DALAM KALANGAN PENJAWAT AWAM

MOHD RAFIZAM BIN MOHAMED

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN DARIPADA SYARAT MEMPEROLEH IJAZAH SARJANA SISTEM MAKLUMAT

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2018

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satu saya telah jelaskan sumbernya.

18 Jun 2018 MOHD RAFIZAM BIN MOHAMED

GP04651

PENGHARGAAN

Syukur Alhamdulillah kepada Allah S.W.T kerana dengan limpah kurniaNya dapat saya menyiapkan kajian ini dengan sempurna dan jayanya. Selawat serta salam kepada junjungan besar Nabi Muhammad SAW serta para keluarga dan sahabat baginda.

Jutaan terima kasih yang tidak terhingga kepada penyelia saya, Dr. Ibrahim Mohamed di atas segala tunjuk ajar, bimbingan, panduan, sokongan, teguran serta nasihat di sepanjang kajian ini dijalankan. Terima kasih juga diucapkan kepada Jabatan Perkhidmatan Awam Malaysia (JPA) di atas tajaan pengajian ini serta semua pensyarah dan warga Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia di atas tunjuk ajar serta bantuan yang telah diberikan di sepanjang pengajian saya.

Rasa terima kasih juga saya panjangkan kepada pihak Ibu Pejabat Suruhanjaya Pilihan Raya Malaysia (SPR) Putrajaya, khususnya Seksyen Teknologi Maklumat atas kerjasama yang diberikan sepanjang kajian ini dijalankan. Terima kasih yang tidak terhingga juga saya ucapkan kepada semua rakan seperjuangan saya sesi 2016/2018 serta rakan-rakan di UKM di atas segala bantuan dan sokongan yang berpanjangan tanpa mengira masa.

Buat isteri tercinta yang amat memahami, Nur Aliah binti Abdullah serta anak-anak tersayang Iwana, Izzati, Irdina dan Muadz, juga buat ibu Siti Maryam binti Nor serta Rokiah binti Awang Nong terima kasih di atas kasih-sayang, kesabaran, kata nasihat, bantuan, sokongan serta dorongan yang diberikan di sepanjang pengajian saya.

ABSTRAK

Tujuan kajian ini dilakukan adalah untuk melihat tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam. Kajian kes dilakukan di salah sebuah agensi sektor awam iaitu Ibu Pejabat Suruhanjaya Pilihan Raya (SPR) Malaysia yang terletak di Putrajaya. Pemilihan SPR sebagai agensi terpilih adalah kerana agensi ini mempunyai maklumat yang penting dan sensitif seperti rekod pendaftaran pemilih, maklumat persempadanan dan rekod pengundi rakyat Malaysia. Berdasarkan kepada kajian dari pengkaji yang lepas, adalah didapati faktor pekerja menyumbang kepada isu keselamatan maklumat. Maka jelaslah bahawa perlu ada kesedaran keselamatan maklumat dalam kalangan penjawat awam yang bertugas di sektor awam bagi melindungi dan menjaga keselamatan maklumat di setiap agensi. Kesedaran keselamatan maklumat penjawat awam diukur dengan merujuk kepada empat faktor yang telah dikenalpasti melalui ulasan kepustakaan yang terdiri daripada faktor sikap, latihan dan pendidikan, sokongan pihak pengurusan dan polisi/dasar keselamatan maklumat. Kaedah kajian ini dimulakan dengan pencarian kajian terdahulu mengenai isu berkaitan kesedaran keselamatan maklumat bagi mencari jurang kajian. Seterusnya, ulasan kepustakaan yang lebih mendalam dilakukan untuk membangunkan instrumen bagi soalan kaji selidik. Borang kaji selidik secara atas talian dan manual digunakan untuk mendapat maklumbalas daripada 132 responden. Perisian *Statistical Package for Social Science* (SPSS) versi 24.0 digunakan untuk tujuan analisis dan dipersembahkan dalam bentuk jadual dan graf bagi mendapatkan keputusan yang dikehendaki. Dapatan kajian menunjukkan tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam untuk faktor yang dikenalpasti adalah di tahap yang baik dan saling berhubungkait. Pada akhir kajian, satu cadangan model telah dibangunkan yang telah mendapat pengesahan daripada pakar yang berpengalaman dan boleh dijadikan sebagai panduan bagi kaedah untuk mempertingkatkan tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam.

MODEL FOR LEVEL OF INFORMATION SECURITY AWARENESS AMONG CIVIL SERVANTS

ABSTRACT

The purpose of this study is to look at the level of information security awareness among civil servants. The case study was conducted at one of the public sector agencies, Malaysia Election Commission (EC) headquarters located in Putrajaya. EC selection as a selected agency is based on this agency which has important and sensitive information such as voter registration records, borders information and the record of Malaysian voters. Based on the previous researcher's findings, it is found that the people factors contributes to the information security issues. It is clear that there needs to be awareness of information security in the workforce, especially among civil servants in the public sector to protect and safeguard the information security in every agency. Awareness of civil servants information security is measured by reference to four factors that have been identified through literature review consisting of attitude, training and education factors, management support and information security policies. The methodology of this study was initiated by looking for a previous study on the issue of information security awareness to find the study gap. Subsequently, a more in-depth literature review was conducted to develop instruments for questionnaires. An online and manual survey form was used to get feedbacks from 132 respondents. Statistical Package for Social Science (SPSS) version 24.0 is used for analysis purposes and is presented in the form of tables and graphs to get the desired results. The findings shows that the level of awareness of information security among civil servants for the identified factors is in good and mutually compatible. At the end of the study, a model proposal has been developed which has been certified by experienced experts and can be used as a guide for ways to improve the level of information security awareness among civil servants.

KANDUNGAN

SENARAI JADUAL

SENARAI ILUSTRASI

SENARAI SINGKATAN

CA	*Cronbach's Coefficient Alpha*
ICT	*Information and Communication Technology*
IS	*Information System*
ISP	*Information Security Policy*
MAMPU	*Malaysian Administrative Modernization and Management Planning Unit*
RAKKSA	*Rangka Kerja Keselamatan Siber Sektor Awam*
SPR	*Suruhanjaya Pilihan Raya*
SPSS	*Statistical Package for the Social Sciences*
TAM	*Technology Acceptance Model*
TPA	*Theory of Planned Behaviour*
TRA	*Theory of Reasoned Action*
UKM	*Universiti Kebangsaan Malaysia*

BAB I

PENDAHULUAN

1.1 PENGENALAN

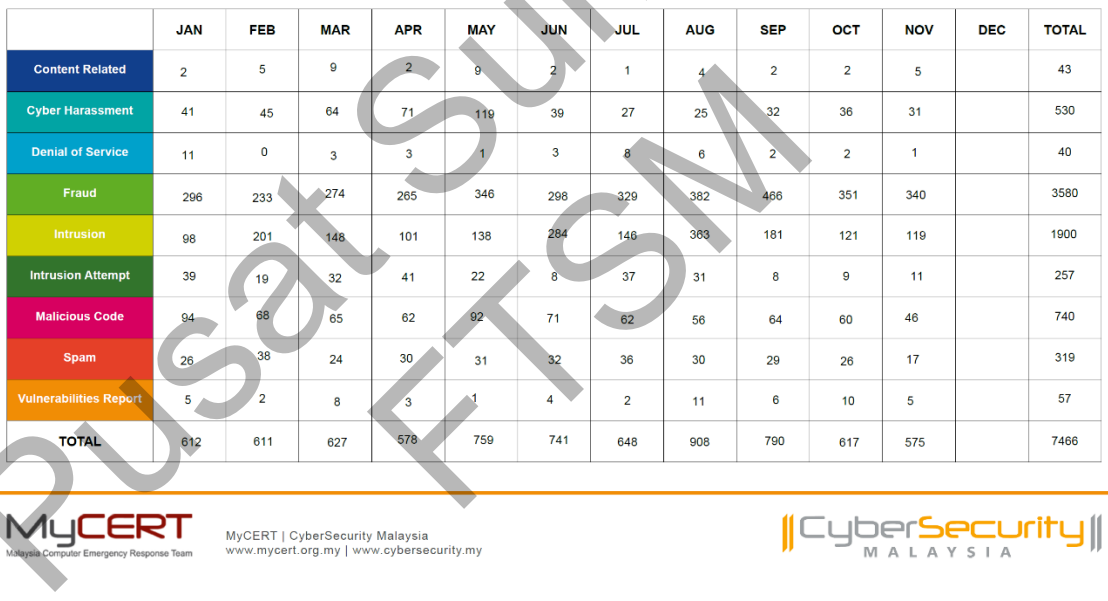
Penggunaan teknologi maklumat dan komunikasi telah mempengaruhi kehidupan manusia dengan ketara pada masa kini. Teknologi berasaskan web telah membawa banyak kelebihan kepada organisasi dan pelanggan tetapi pelanggaran keselamatan maklumat masih menjadi kebimbangan di setiap agensi kerajaan. *Anti-virus, anti-malware, anti-spam, anti-phishing, anti-spyware, firewall*, dan sistem pengesanan pencerobohan adalah antara aspek teknologi yang digunakan untuk menangani keselamatan maklumat, tetapi teknologi ini tidak dapat menjamin persekitaran yang selamat untuk perlindungan maklumat (Safa et al. 2015).

Keselamatan maklumat masih merupakan isu penting bagi kedua-dua pengguna dan organisasi. Teknologi tidak semata-mata menjamin persekitaran yang selamat untuk maklumat; aspek manusia bagi menjamin keselamatan maklumat harus dipertimbangkan, selain aspek teknologi. Kekurangan kesedaran keselamatan maklumat, kejahilan, kecuaian, sikap tidak peduli, kerosakan, dan ketahanan adalah asas kesalahan yang dilakukan oleh ramai pekerja (Safa et al. 2016).

Di Malaysia, agensi kerajaan juga turut digesa untuk meningkatkan tahap kecekapan dan keberkesanan mengawal ancaman luar yang boleh mengugat isu keselamatan maklumat (MAMPU 2016). Walaupun terdapat kelebihan dari segi penyampaian maklumat kepada orang ramai dengan menggunakan perkhidmatan atas talian, namun agensi juga terdedah kepada risiko keselamatan melalui penggantungan kepada penggunaan teknologi maklumat dan komunikasi untuk menjalankan perkhidmatan mereka, khususnya organisasi yang menawarkan perkhidmatan atas talian. Terdapat pelbagai langkah yang diambil oleh pihak kerajaan bagi menangani

masalah keselamatan maklumat. Antara yang terkini adalah, pihak *Malaysian Administrative Modernization and Management Planning Unit* (MAMPU) telah mengeluarkan satu rangka kerja keselamatan siber sektor awam (RAKKSA) bertujuan memberi panduan asas serta merangkumi kesemua komponen keselamatan yang perlu diambil kira oleh kementerian dan agensi sektor awam untuk melindungi maklumat dalam ruang siber mereka.

Menurut statistik yang dikeluarkan oleh MyCert pada tahun 2017 (Rajah 1.1), terdapat 7,466 kes insiden keselamatan yang telah berlaku sehingga November 2017. Rajah 1.1 menunjukkan statistik pelbagai jenis insiden keselamatan maklumat dari Januari hingga November 2017.



	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	2	5	9	2	9	2	1	4	2	2	5		43
Cyber Harassment	41	45	64	71	119	39	27	25	32	36	31		530
Denial of Service	11	0	3	3	1	3	8	6	2	2	1		40
Fraud	296	233	274	265	346	298	329	382	466	351	340		3580
Intrusion	98	201	148	101	138	284	146	363	181	121	119		1900
Intrusion Attempt	39	19	32	41	22	8	37	31	8	9	11		257
Malicious Code	94	68	65	62	92	71	62	56	64	60	46		740
Spam	26	38	24	30	31	32	36	30	29	26	17		319
Vulnerabilities Report	5	2	8	3	1	4	2	11	6	10	5		57
TOTAL	612	611	627	578	759	741	648	908	790	617	575		7466

Rajah 1.1 Statistik Insiden Keselamatan Maklumat Tahun 2017
(Sumber : https://www.mycert.org.my/statistics/2017.php)

Oleh yang demikian, bagi memastikan keselamatan maklumat adalah bebas daripada ancaman virus, serangan pengodam, cacing *(worm), spam* dan sebagainya maka keperluan untuk meningkatkan kesedaran keselamatan maklumat dalam kalangan penjawat awam perlu dititikberatkan. Justuru itu, selain menyediakan polisi dan dasar

berkaitan keselamatan maklumat, usaha untuk mempertingkatan kesedaran keselamatan maklumat dalam kalangan penjawat awam adalah perlu dilakukan bagi memelihara keselamatan maklumat dalam agensi kerajaan.

1.2 LATAR BELAKANG

Menurut Da Veiga & Martins (2015), kawalan keselamatan maklumat memberi impak terhadap proses organisasi, teknologi dan cara memproses maklumat pekerja. Untuk melaksanakan amalan keselamatan maklumat secara berkesan, organisasi mesti memastikan bahawa budaya itu kondusif untuk melindungi maklumat. Menanamkan budaya di mana maklumat ditadbir dan dilindungi oleh semua pekerja pada setiap masa mengikut dasar organisasi dan keperluan pengawalseliaan bukanlah satu tugas yang mudah. Adalah penting untuk memahami persepsi, sikap dan tingkah laku pekerja organisasi untuk membentuk budaya keselamatan maklumat menjadi satu di mana sifat, kerahsiaan dan kepekaan maklumat difahami, dan maklumat dikendalikan dengan sewajarnya.

Perlindungan maklumat dan perlindungan data menjadi kebimbangan dan cabaran penting yang dihadapi organisasi dan pengguna. Walaupun usaha dan wang yang dibelanjakan oleh organisasi untuk menjamin keselamatan maklumat, banyak kejadian pelanggaran data dan kehilangan maklumat terus berlaku setiap tahun. Hari ini, organisasi menyedari bahawa mengawal keselamatan maklumat adalah tugas yang berterusan dan kompleks (Metalidou et al. 2014).

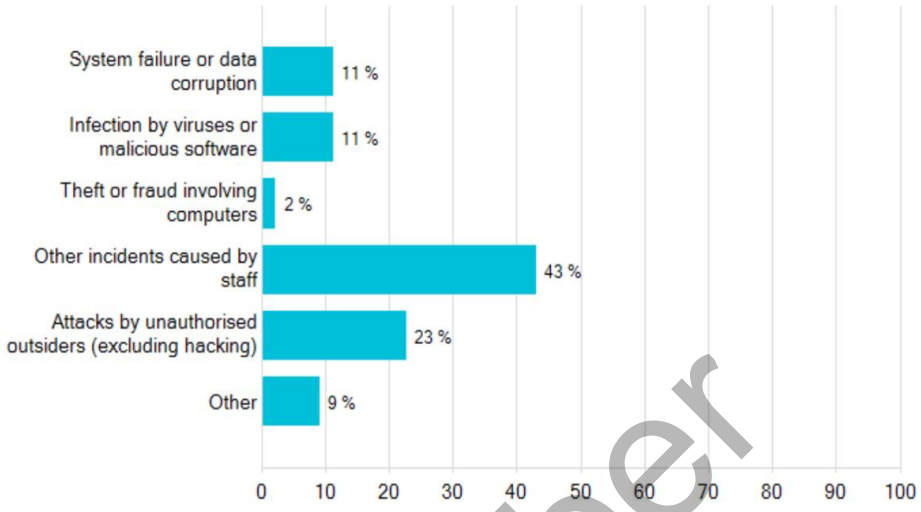
Beban menyimpan maklumat yang selamat terletak pada bahu semua fungsi organisasi dan ahli. Oleh itu, pengguna mesti sedar akan peranan dan tanggungjawab mereka dalam melindungi maklumat dan bagaimana untuk bertindak balas terhadap sebarang ancaman yang berpotensi. Seterusnya, program kesedaran keselamatan harus memberi tumpuan kepada pengguna yang memberi pendedahan tentang bagaimana untuk melindungi maklumat dengan berkesan (Al-Omari et al. 2013).

Pembangunan pesat dan inovasi dalam teknologi digital memberikan banyak faedah kepada kehidupan manusia, tetapi ia juga tidak terlepas daripada kesan negatif misalnya jenayah siber. Dalam era digital yang pesat dan cepat berubah, Internet kini menjadi amalan dalam kehidupan seharian. Walau bagaimanapun, ia telah mewujudkan banyak isu mengenai keselamatan maklumat. Ini termasuk isu-isu ke arah kecurian dan penyalahgunaan maklumat peribadi atau maklumat organisasi. Keselamatan maklumat tidak lagi dapat dipulihkan melalui teknologi itu sendiri tetapi sebahagiannya, dan kebanyakannya dicapai melalui penggunaan Internet yang selamat dalam kalangan pengguna (Aloul 2012).

Pada masa lalu, penyelidikan mengenai keselamatan maklumat memberi tumpuan kepada isu teknikal dan penyelesaian teknikal telah dibangunkan untuk menangani penafian serangan perkhidmatan kepada sistem pengkomputeran, *malware*, serangan pencerobohan, *spoofing*, serangan katalaluan, penyaduran dan lain-lain. Walau bagaimanapun, dalam tahun-tahun kebelakangan ini, telah diakui bahawa faktor manusia memainkan peranan penting dalam banyak kegagalan keselamatan maklumat (Furnell & Thomson 2009).

Bulgurcu et al. (2010) telah mentakrifkan kesedaran keselamatan maklumat sebagai pengetahuan umum para pekerja mengenai keselamatan maklumat dan kesedaran mereka tentang *ISP* di dalam organisasi. Kesedaran keselamatan maklumat merupakan faktor penting kerana ia dapat memastikan pengguna mengetahui risiko keselamatan dan mengamalkan tingkah laku keselamatan yang disyorkan (Rezgui & Marks 2008). Kajian terdahulu mendapati bahawa ramai pekerja mempunyai kesedaran dan pemahaman penggunaan yang rendah tentang keselamatan maklumat (Brady 2011; Höne, & Eloff 2002) dan ia juga merupakan salah satu komponen keselamatan maklumat yang kritikal (Al-Omari, & El-Gayar 2012; Kim 2014).

Satu kajian yang telah dijalankan oleh PricewaterhouseCoopers (PwC) pada tahun 2015, telah mendapati 43% insiden yang melibatkan pelanggaran keselamatan maklumat adalah disebabkan oleh pekerja (Rajah 1.2).



Rajah 1.2 Keputusan Penyelidikan Keselamatan Siber 2015
(Sumber : https://dm.pwc.com/HMG2015BreachesSurvey/)

Perhatian yang serius perlu diberi terhadap kepentingan membina kesedaran keselamatan maklumat bagi memastikan bahawa kemalangan keselamatan maklumat dapat dielakkan. Walaupun terdapat langkah yang diambil untuk melindungi keselamatan data seperti penggunaan *firewall* bagi menangkis serangan pihak luar, penggunaan perisian *antivirus* untuk mengelakkan serangan *malware* dan polisi keselamatan yang lengkap untuk rujukan keselamatan maklumat, namun keberkesanan langkah tersebut adalah kurang sekiranya pekerja yang berurusan dengan maklumat tidak mempunyai kesedaran betapa pentingnya melindungi maklumat terutamanya apabila melibatkan rahsia organisasi.

1.3 PENYATAAN MASALAH

Kesedaran keselamatan maklumat di kalangan pekerja adalah sangat penting di dalam organisasi kerana ia berupaya untuk mengurangkan kejadian insiden keselamatan (Al-Omari et al. 2013; Eminağaoğlu, Uçar & Eren 2009). Beberapa kajian melaporkan bahawa ancaman keselamatan maklumat yang utama di dalam sesebuah organisasi adalah ancaman dalaman daripada pekerja (Safa et al. 2016; Siponen, Adam Mahmood & Pahnila 2014).

Para pekerja ini mempunyai akses yang sah dan kerap mendapat kelebihan untuk kemudahan dan maklumat organisasi, pengetahuan tentang organisasi, prosesnya dan mengetahui lokasi aset kritikal atau berharga (Colwill 2009). Justeru itu, banyak organisasi kini menyedari mengenai keperluan untuk melabur bukan sahaja di dalam aspek teknikal sistem tetapi juga di dalam aspek sumber manusia.

Tambahan pula, menurut Ahlan et al. (2011), kekurangan kesedaran keselamatan maklumat di kalangan pekerja berlaku kerana mereka tidak memahami sepenuhnya tentang kepentingan maklumat organisasi mereka. Dengan itu, para pekerja memberi keutamaan yang kurang terhadap keselamatan maklumat.

Samy et al. (2010) mendedahkan bahawa lima kategori ancaman yang paling kritikal terhadap keselamatan maklumat adalah kegagalan kuasa (contohnya, kegagalan pelayan dan gangguan penyedia perkhidmatan), kesilapan manusia (misalnya kemasukan data yang salah oleh pekerja dan penghapusan secara tidak sengaja atau pengubahsuaian data oleh pekerja), teknologi usang (misalnya perkakasan dan pemasangan perisian yang ketinggalan zaman), kegagalan perkakasan (contohnya kesalahan penyelenggaraan perkakasan), dan kegagalan perisian (contohnya kesalahan penyelenggaraan perisian).

Isu yang berkaitan dengan teknologi boleh diuruskan dengan mudah oleh organisasi. Walau bagaimanapun, isu kesilapan manusia boleh menjadi rumit dan mencabar (Al-Omari et al. 2013; Ifinedo 2014; Liginlal, Sim & Khansa 2009; Safa et al. 2015; Sarkar 2010). Para penyelidik dalam kajian terdahulu telah menyarankan bahawa organisasi perlu melabur lebih banyak modal insan daripada teknologi itu sendiri. Ini kerana kebanyakan insiden keselamatan adalah disebabkan oleh kecuaian dan kurangnya kebolehan para pekerja dalaman di dalam menggunakan alat keselamatan dengan betul (Akhunzada et al. 2015; Parsons et al. 2014).

Selain itu, banyak insiden keselamatan yang dilaporkan di dalam kajian terdahulu adalah disebabkan oleh para pekerja dalaman kerana kurangnya kesedaran keselamatan (Al-Omari et al. 2013; Albrechtsen, & Hovden 2010; Aurigemma, & Panko 2012; Brady 2011; Herath, & Rao 2009). Ramai penyelidik dan pakar dalam

bidang keselamatan maklumat menegaskan bahawa pengguna adalah sasaran yang paling lemah dalam rangkaian apabila ia berkaitan dengan keselamatan maklumat dan aset keselamatan sesebuah organisasi (Metalidou et al. 2014). Kesalahan manusia masih merupakan perkara utama yang mungkin mengancam dan merosakkan aset organisasi. Akibatnya, cabaran bagi kebanyakan organisasi hari ini adalah untuk meningkatkan kesedaran keselamatan maklumat kepada para pekerja mereka sendiri.

Berdasarkan kepada kajian dari pengkaji yang lepas, adalah didapati faktor pekerja menyumbang kepada isu keselamatan maklumat. Maka jelaslah bahawa perlu ada kesedaran keselamatan maklumat dalam pekerja terutamanya kalangan penjawat awam yang bertugas di sektor awam bagi melindungi dan menjaga keselamatan maklumat. Kajian ini perlu dilakukan untuk melihat faktor-faktor yang mempengaruhi tahap kesedaran maklumat dalam kalangan penjawat awam dan membangunkan model yang dapat membantu mempertingkatkan kesedaran keselamatan maklumat dalam kalangan penjawat awam.

1.4 OBJEKTIF KAJIAN

Kajian ini secara spesifiknya menggariskan dua (2) objektif utama iaitu:

a) Mengenalpasti faktor dan hubungan kesedaran keselamatan maklumat dalam kalangan penjawat awam.
b) Membangunkan model kesedaran keselamatan maklumat dalam kalangan penjawat awam.

1.5 PERSOALAN KAJIAN

Berdasarkan objektif yang telah digariskan, kajian ini akan menjawab dua (2) persoalan utama iaitu:

a) Apakah wujud hubungan faktor dan kesedaran keselamatan maklumat dalam kalangan penjawat awam?
b) Apakah model kesedaran keselamatan maklumat dalam kalangan penjawat awam yang boleh dibangunkan?

1.6 SKOP DAN BATASAN KAJIAN

Skop dan batasan kajian ini adalah seperti berikut:

a) Kajian ini melibatkan penjawat awam di Ibu pejabat Suruhajaya Pilihan Raya Malaysia (SPR) Putrajaya yang merupakan kajian kes.
b) Pemilihan SPR adalah berdasarkan kepada agensi ini yang mempunyai maklumat yang penting dan sensitif seperti rekod pendaftaran pemilih, maklumat persempadanan dan rekod pengundi rakyat Malaysia.
c) Kajian ini mengandaikan bahawa semua responden yang dipilih mempunyai hak capaian yang sama ke atas capaian rangkaian komputer yang menjadi asas kajian.
d) Terdapat seramai 200 penjawat awam yang bertugas di SPR dan saiz sampel adalah terhad kepada 132 responden sahaja berdasarkan rujukan yang di rujuk kepada (Krejcie, & Morgan 1970).

1.7 KEPENTINGAN KAJIAN

Kepentingan kajian ini adalah seperti berikut:

(i) Meningkatkan budaya kerja yang lebih baik, serta menerapkan kesedaran tentang betapa pentingnya amalan keselamatan maklumat di tempat kerja.
(ii) Memberikan sumbangan kepada sesiapa yang terlibat secara langsung dengan teknologi maklumat dan komunikasi sebagai garis panduan dalam mempertingkatkan lagi peraturan-peraturan dan amalan keselamatan

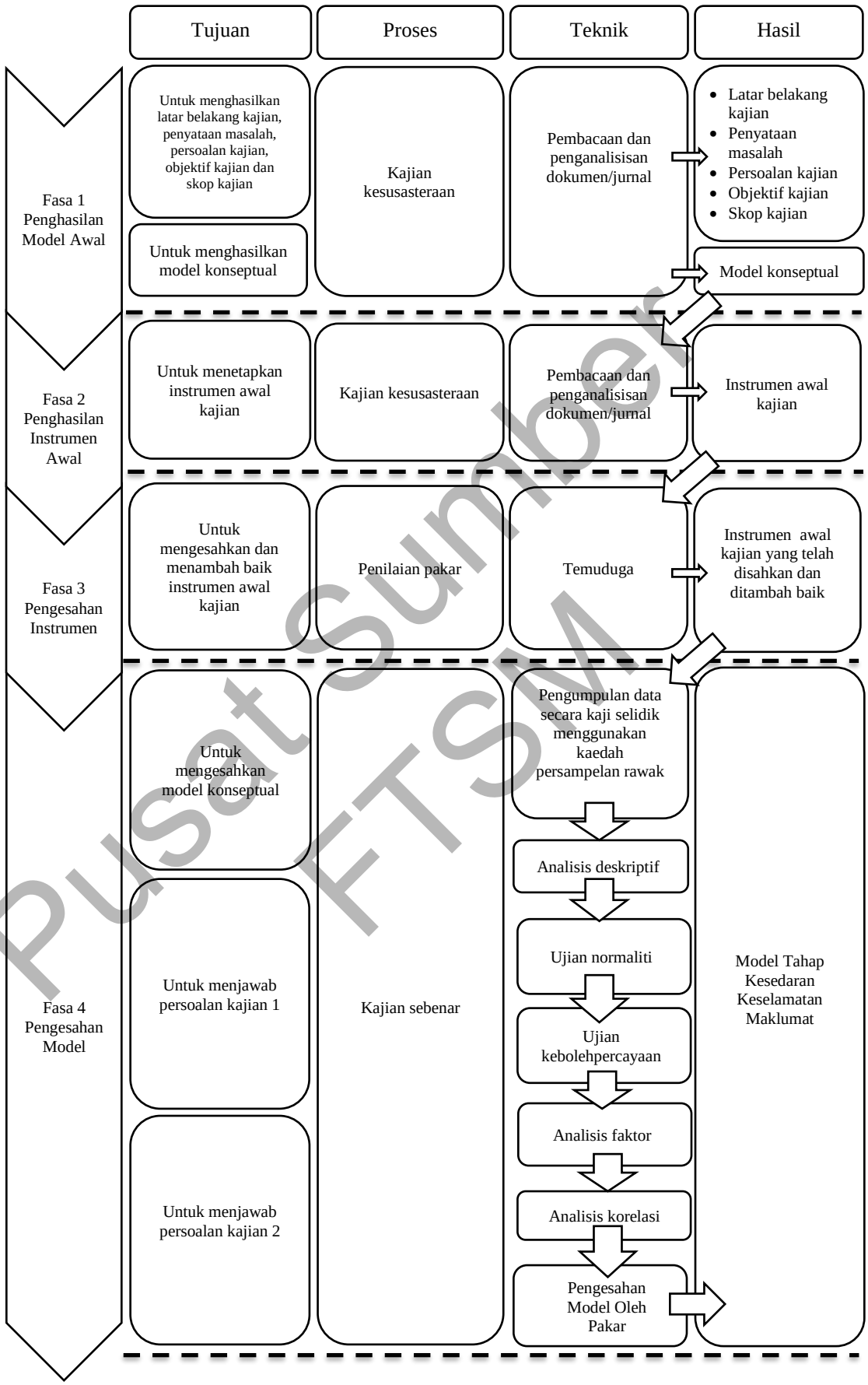
maklumat sedia ada dan seterusnya meningkatkan amalan budaya kerja yang selamat.

(iii) Memberikan sumbangan dan panduan kepada pihak jabatan kerajaan dalam proses penambahbaikkan pengendalian keselamatan maklumat.

Dengan adanya kajian ini, sektor awam dapat membuat penilaian dan penambah baikan berterusan ke atas tahap kesedaran keselamatan maklumat bagi memastikan produktiviti penyampaian perkhidmatan awam terus meningkat. Kajian ini adalah penting kerana ia mampu mewujudkan satu model yang komprehensif kepada sektor awam untuk menilai tahap kesedaran kesedaran keselamatan maklumat dalam kalangan penjawat awam.

1.8 PENDEKATAN KAJIAN

Pendekatan kajian terdiri daripada empat (4) fasa utama iaitu penghasilan model konseptual, penghasilan instrumen awal, pengesahan instrumen awal dan pengesahan model. Setiap fasa diperincikan kepada proses-proses yang terlibat, tujuan pelaksanaan setiap proses, teknik yang digunakan bagi setiap proses dan hasil akhir bagi setiap proses. Gambaran pendekatan kajian adalah seperti yang ditunjukkan dalam Rajah 1.3.



Rajah 1.3 Pendekatan kajian

1.9 STRUKTUR PENULISAN

Struktur penulisan bagi kajian ini dibahagikan kepada lima (5) bab utama seperti berikut:

a) **Bab I** terdiri daripada pengenalan, latar belakang, penyataan masalah, objektif kajian, persoalan kajian, skop dan batasan kajian, kepentingan kajian dan pendekatan kajian.

b) **Bab II** mengandungi kajian kesusasteraan yang dibuat terhadap kajian terdahulu dalam bidang keselamatan maklumat iaitu faktor kesedaran keselamatan maklumat.

c) **Bab III** menerangkan secara sistematik pendekatan kajian yang digunakan untuk mencapai objektif kajian dan juga menjawab persoalan kajian. Bab ini menerangkan secara terperinci proses-proses yang terlibat seperti penghasilan model awal konseptual, penghasilan instrumen awal kajian, pengesahan instrumen kajian dan akhir sekali pengesahan model kajian.

d) **Bab IV** membincangkan hasil analisis secara statistikal dan analitikal bagi data yang dikumpul melalui kaji selidik yang diedarkan kepada responden yang terpilih.

e) **Bab V** merupakan kesimpulan kepada kajian, sumbangan kajian dan cadangan penambahbaikan kajian ini pada masa hadapan.

1.10 KESIMPULAN

Bab ini memberi gambaran tentang kajian yang melibatkan tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam di jabatan kerajaan. Berdasarkan huraian yang diterangkan dalam bab ini, pembaca diharap lebih mudah untuk memahami kajian yang dijalankan ini. Pernyataan masalah pula mengupas

tentang senario semasa yang mendorong kepada kajian tentang tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam.

Kajian ini juga diharap dapat membantu penjawat awam di setiap agensi kerajaan dalam meningkatkan budaya kerja yang lebih baik, serta menerapkan pemahaman tentang betapa pentingnya kesedaran keselamatan maklumat semasa mengendalikan urusan kerja seharian di setiap agensi kerjaan yang menggunakan teknologi komputer.

Dapatan kajian juga diharapkan dapat menyumbang kepada peningkatan kesedaran keselamatan maklumat dalam kalangan penjawat awam sama ada yang bertugas secara langsung atau tidak langsung di bidang yang berkaitan dengan teknologi komputer. Seterusnya, penyampaian perkhidmatan kepada orang ramai dapat dilakukan dengan selamat dan berkesan.

BAB II

KAJIAN KESUSASTERAAN

2.1 KESELAMATAN MAKLUMAT

Menurut takrifan *Malaysian Administrative Modernization and Management Planning Unit* MAMPU (2010), maklumat merupakan hasil terakhir sesuatu sistem pengkomputeran dan dengan itu ianya amat penting dan bernilai bagi sesebuah organisasi. Kehilangan atau kemusnahan data/maklumat yang disimpan di dalam komputer sering berlaku disebabkan oleh kejadian seperti kebakaran, pengkhianatan, kecuaian dan kecurian. Bagi mengatasi masalah ini, kawalan ke atas capaian data/ maklumat dan keselamatan fizikal perlu diperketatkan.

Disamping itu data atau maklumat yang penting perlu dibuat salinan yang secukupnya dan disimpan di bangunan berasingan. Data atau maklumat yang dicuri melalui talian komunikasi data dapat dicegah dengan teknik yang lebih rumit misalnya dengan menggunakan kaedah penyulitan *(encryption).* Manakala, keselamatan teknologi maklumat dan komunikasi merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin kerahsiaan, integriti, kesahihan dan kebolehsediaan kepada semua pengguna yang dibenarkan.

Keselamatan maklumat pula ditakrifkan sebagai perlindungan sistem maklumat daripada ancaman akses dan maklumat yang tidak dibenarkan (Cavalli et al. 2004; Tamjidyamcholo et al. 2013). Keselamatan maklumat adalah salah satu unsur penting yang perlu dipertimbangkan dalam pembangunan sistem maklumat. Banyak organisasi telah pun melaksanakan teknologi keselamatan canggih seperti kad pintar dan biometrik bagi memantapkan keselamatan maklumat organisasi (Kreicberga 2010).

Menurut Lebek et al. (2013), isu keselamatan maklumat adalah isu utama dalam

agensi kerajaan kerana banyak maklumat penting yang perlu dipelihara bagi kepentingan awam. Maklumat kerajaan adalah sangat sensitif dan sulit, oleh itu data memerlukan perlindungan keselamatan kerana jika maklumat kerajaan terdedah kepada pengguna yang tidak dibenarkan, ia mungkin menjejaskan kredibiliti sesebuah kerajaan. Manakala menurut Brady (2011) pula, keselamatan maklumat adalah program yang membolehkan organisasi untuk melindungi persekitaran yang saling berkait rapat dari kelemahan sistem, serangan, ancaman, dan insiden.

Siponen et al. (2014) pula menjelaskan bahawa keselamatan maklumat merupakan suatu cara kerja untuk melindungi aset maklumat tanpa mengira keadaan maklumat tersebut sama ada sedang digunakan, disimpan atau dalam proses penghantaran. Keselamatan maklumat tidak hanya tertumpu kepada sesuatu teknologi sahaja, sebaliknya ia merupakan suatu strategi yang terdiri daripada proses serta penggunaan alatan dan dasar polisi yang sesuai untuk mencegah atau mengesan ancaman maklumat fizikal atau digital.

Walau bagaimanapun, teknologi ini tidak dapat menjanjikan keselamatan sistem maklumat yang berkesan sekiranya tingkah laku keselamatan maklumat pekerja dalam organisasi tidak dapat diterima. Para pekerja atau pengguna sistem maklumat sebenarnya merupakan garis pertahanan utama dan paling kritis (Eminağaoğlu et al. 2009). Idea ini juga disokong oleh kajian lain yang menyatakan bahawa pekerja adalah faktor utama sama ada kejayaan atau kegagalan keselamatan sistem maklumat dalam mana-mana organisasi (Ahlan et al. 2011).

Kerajaan melalui agensi pelaksana MAMPU (MAMPU 2010) menakrifkan keselamatan maklumat sebagai keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem teknologi maklumat dan komunikasi berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan maklumat berkait rapat dengan perlindungan aset teknologi maklumat dan komunikasi. Terdapat empat (4) komponen asas keselamatan teknologi maklumat dan komunikasi iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(d) Memastikan akses kepada hanya pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

2.2 ANCAMAN KESELAMATAN MAKLUMAT

Ancaman ditakrifkan sebagai sebarang penyebab kepada kejadian yang dijangka dan diluar jangka yang memberi impak negatif kepada sistem atau organisasi (Samy et al. 2010). Ancaman keselamatan maklumat adalah serius dan harus dikawal dan diawasi oleh organisasi kerana ia berpotensi menyebabkan bahaya (Alhabeeb et al. 2010). Ancaman keselamatan maklumat boleh dibahagikan kepada dua jenis: ancaman luaran dan ancaman dalaman.

Ancaman luar disebabkan oleh orang luar di mana ia mudah dikawal menggunakan teknologi keselamatan seperti *firewall* (Safa et al. 2016; Colwill 2009). Ancaman dalaman boleh jadi berniat jahat (pekerja yang merancang untuk membalas dendam dan keuntungan kewangan) atau tidak berniat jahat (kesalahan manusia) (Sarkar 2010). Ini adalah kerana mereka mempunyai akses yang sah dan kerap mendapat akses kepada kemudahan dan maklumat organisasi. Mereka juga mempunyai pengetahuan tentang organisasi dan prosesnya, dan mengetahui lokasi aset kritikal atau berharga (Colwill 2009).

Banyak organisasi tidak menyedari bahawa ancaman dalaman boleh menyebabkan kemudaratan seperti mencuri dan memusnahkan maklumat organisasi boleh menyebabkan insiden keselamatan yang tidak diingini. Selain itu, menurut Sarkar (2010), serangan oleh orang dalam sukar untuk dikesan berbanding dengan aktiviti daripada pihak luar. Oleh itu, organisasi perlu bersedia untuk melabur lebih banyak

pembangunan modal insan berbanding perbelanjaan teknologi sahaja dalam memerangi ancaman keselamatan maklumat (Da Veiga & Martins 2015; Krugerv& Kearney 2006). Pekerja atau pengguna tanpa pendidikan dan pengetahuan yang betul mengenai keselamatan maklumat, mereka tidak akan dapat mempraktikkannya dengan tepat (Safa et al. 2015; Shropshire, Warkentin & Sharma 2015).

Klasifikasi ancaman keselamatan maklumat adalah luas di dalam literatur keselamatan teknologi maklumat dan komunikasi. Guo (2013) membahagikan ancaman keselamatan maklumat kepada empat dimensi; (i) sumber, yang boleh menjadi dalaman atau luaran kepada organisasi yang berkenaan; (ii) pelaku, yang boleh menjadi manusia atau bukan manusia; (iii) niat, yang boleh disengajakan atau tidak disengajakan; dan (iv) akibat, yang boleh menjadi pendedahan, pengubahsuaian, pemusnahan, atau penolakan perkhidmatan. Ancaman juga boleh dilakukan secara tidak disengajakan atau sengaja (Jung et al. 2001). Ancaman tidak sengaja boleh menjadi bencana alam dan kesilapan manusia atau terlepas pandang, manakala ancaman yang disengaja adalah tindakan seperti penipuan komputer, penyelewengan, dan kecurian.

Manakala, MAMPU (2010) menakrifkan insiden keselamatan maklumat sebagai musibah (*adverse event*) yang berlaku ke atas aset teknologi maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan teknologi maklumat dan komunikasi sama ada yang ditetapkan secara tersurat atau tersirat.

2.3 KESEDARAN KESELAMATAN MAKLUMAT

Kesedaran keselamatan maklumat merujuk kepada pemahaman para pekerja mengenai kepentingan keselamatan maklumat, keupayaan untuk mengiktiraf ancaman keselamatan maklumat dan tanggungjawab mereka untuk mengamalkan tingkah laku keselamatan dengan betul untuk melindungi data organisasi (Shaw et al. 2009; Rezgui & Marks 2008).

Bulgurcu et al. (2010) menyatakan kesedaran keselamatan maklumat sebagai pengetahuan umum para pekerja tentang keselamatan maklumat dan kesedaran mereka terhadap ISP organisasi. Wang (2012) berhujah bahawa kesedaran dan pengalaman keselamatan adalah sebahagian daripada pengetahuan keselamatan maklumat individu.

Sekiranya para pekerja mempunyai hanya sedikit pengetahuan mengenai keselamatan maklumat, mereka mungkin tidak menyedari betapa pentingnya mematuhi dan mengamalkan ISP organisasi. Selain itu, Boss et al. (2009) menyatakan bahawa, untuk seseorang pekerja itu mematuhi dasar dan prosedur keselamatan, dia seharusnya sedar mengenai ancaman keselamatan.

Kesedaran keselamatan maklumat di kalangan pekerja bukan hanya meliputi pengetahuan umum tentang kesedaran keselamatan, tetapi pekerja harus mempunyai pengetahuan dan kesedaran mengenai keparahan dan kerentanan terhadap ancaman keselamatan serta faedah alat keselamatan yang dapat digunakan untuk mengurangkan ancaman keselamatan.

Kesilapan manusia dan tingkah laku yang bermasalah dapat dikurangkan jika kesedaran keselamatan pekerja meningkat (Parsons et al. 2014; Shaw et al. 2009). Oleh itu, organisasi perlu membuat kesedaran keselamatan maklumat di kalangan pekerja sebagai satu keutamaan dengan menganjurkan program latihan keselamatan dan kesedaran maklumat (Cheng et al. 2013). Program latihan keselamatan dan kesedaran maklumat perlu dilaksanakan dengan betul kerana ia dapat membantu meningkatkan lagi pengetahuan pekerja.

Safa et al. (2015) juga menyatakan bahawa program kesedaran keselamatan harus relevan dan konsisten kerana kedua-duanya adalah kunci kejayaan di dalam kesedaran keselamatan maklumat. Selain itu, Kreicberga (2010) menyatakan bahawa pengetahuan pekerja dan pengalaman mereka juga dapat dibangunkan berdasarkan kelakuan atasan mereka dan rakan sekerja yang lain.

Oleh itu, pihak pengurusan mesti memberi sokongan penuh dan membina persekitaran positif dalam organisasi untuk memastikan semua pekerja mematuhi

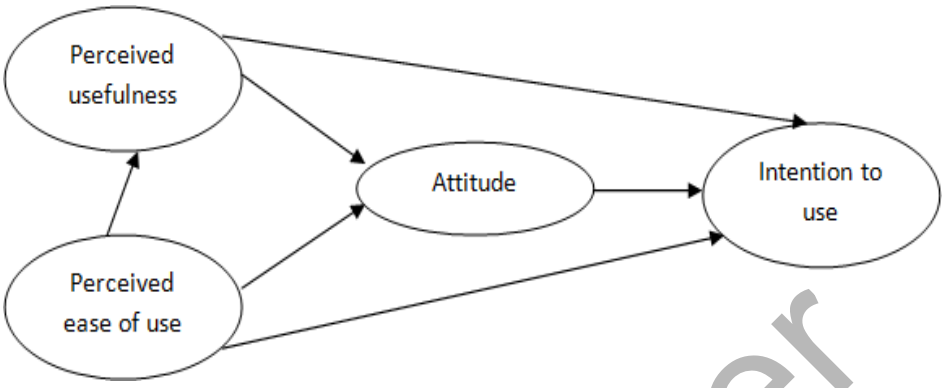
peraturan dan peraturan organisasi menerusi program kesedaran keselamatan maklumat.

2.4 TEORI MODEL KESEDARAN KESELAMATAN MAKLUMAT

Beberapa teori telah dikaji semula untuk mencari teori yang paling sesuai untuk disesuaikan dan kemudian terus dikembangkan menjadi model kajian. Ulasan kesusasteraan sebelumnya mendedahkan beberapa teori yang menyiasat tingkah laku pengguna terhadap teknologi maklumat, di antaranya adalah seperti Model Penerimaan Teknologi (TAM) dan Teori Perancangan yang Dirancang (TPB).

2.4.1 Teori Model Penerimaan Teknologi (TAM)

Model Penerimaan Teknologi (TAM) diadaptasi daripada Teori Aksi Bertindak (TRA) dan telah digunakan dalam banyak kajian untuk menyiasat niat pengguna untuk menggunakan teknologi maklumat. TAM adalah model yang terkenal berdasarkan dua kepercayaan asas: kegunaan terlihat (PU), dan kemudahan penggunaan (PEOU) (Davis 1989; Egea & Gonzalez 2011) untuk menentukan sikap pengguna dan niat tingkah laku untuk menggunakan sistem seperti yang ditunjukkan dalam Rajah 2.1.



Rajah 2.1 : Teori Model Penerimaan Teknologi

PU berhubung dengan kepercayaan pengguna bahawa penggunaan teknologi akan meningkatkan prestasi kerja mereka, sedangkan PEOU merujuk kepada bagaimana pengguna percaya bahawa menggunakan sistem tertentu akan mengurangkan usaha dan masa mereka (Davis 1989). TAM telah digunakan secara meluas dalam kajian berkaitan e-dagang (Kim et al. 2008) dan sistem e-pembelajaran (Shen et al. 2006). Kajian terdahulu menunjukkan bahawa PU dan PEOU menyumbang kepada tingkah laku pengguna terhadap penerimaan teknologi maklumat (Kim et al. 2010; Shen et al. 2006). Al-Omari et al. (2012b) menyesuaikan model TAM dalam kajian mereka untuk menyiasat tingkah laku pematuhan pengguna terhadap ISP. Kajian mendapati kedua-dua PU dan PEOU mempengaruhi pengguna untuk mematuhi ISP organisasi.

Pengguna akan mempunyai niat untuk mengguna pakai teknologi keselamatan jika keselamatan teknologi maklumat berguna, mudah digunakan dan jika mereka merasakan bahawa teknologi akan meningkatkan prestasi kerja mereka (Al-Omari et al. 2012b). Teknologi keselamatan merupakan elemen penting dalam pembangunan teknologi maklumat, dan oleh itu, ia boleh menjadi salah satu faktor yang mempengaruhi pengguna untuk mematuhi ISP organisasi. Teknologi keselamatan

adalah satu kaedah untuk mencegah ancaman keselamatan maklumat, baik dalaman dan luaran.

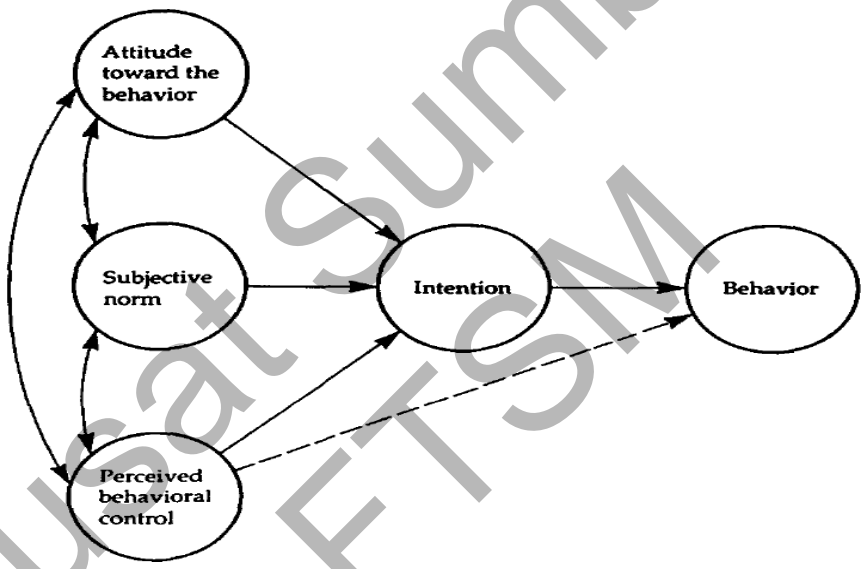
Walau bagaimanapun, alat ini hanya baik untuk menghalang ancaman luar, dan bukan ancaman dalaman (Doherty et al. 2011). Di samping itu, 'kata laluan' sebagai salah satu kaedah yang biasa digunakan merupakan kelemahan yang telah dikenalpasti disebabkan oleh kelakuan pengguna (Parsons et al. 2014; Vu et al. 2007). Sebagai contoh, ramai pengguna gagal menggunakan kata laluan yang kuat, menyebabkan perlindungan keselamatan yang rendah. Kebanyakan mereka juga tidak mengemas kini perisian anti-virus mereka atau mengimbas komputer mereka dengan kerap.

Workman et al. (2008) menyatakan bahawa kebanyakan pekerja merasakan bahawa teknologi keselamatan membosankan dan memakan masa. Oleh itu, mereka biasanya tidak mematuhi ISP, dan sebagai akibatnya, kelemahan data organisasi meningkat. Berdasarkan ulasan kesusasteraan, kajian semasa menunjukkan bahawa pengurusan organisasi perlu melabur lebih banyak perbelanjaan kepada manusia daripada teknologi sahaja dalam memerangi ancaman keselamatan maklumat kerana jika manusia tidak mengguna teknologi dengan betul, insiden keselamatan maklumat akan tetap berlaku (Warkentin et al . 2011).

2.4.2 Teori Perancangan yang Dirancang (TPB)

Teori Perancangan yang Dirancang (TPB) adalah satu lagi teori kelakuan manusia yang dicadangkan oleh Ajzen (1985). TPB yang telah digunakan secara meluas untuk memeriksa penerimaan pengguna sistem maklumat, yang direka untuk meramalkan tingkah laku manusia (Liao et al. 2007). Teori ini juga telah disesuaikan dalam bidang kajian lain yang berkaitan dengan peraturan yang berkaitan dengan tingkah laku pematuhan di kalangan orang (Seppo et al. 2007).

Dalam kajian ini, para penyelidik memberi tumpuan kepada sumber-sumber lain yang harus diberikan oleh organisasi untuk meningkatkan keupayaan dan kemahiran pekerja, seperti dalam melaksanakan mekanisme keselamatan dan latihan keselamatan, yang bertujuan untuk mengawal selia dan mendidik pekerja untuk berperilaku sesuai dengan keselamatan maklumat. Program pendidikan dan latihan dapat meningkatkan kesedaran keselamatan maklumat pengguna (Puhakainen 2006) dan meningkatkan kemahiran pengguna untuk menggunakan alat keselamatan (Koskosas et al., 2011) yang akan membawa kepada peningkatan tingkah laku pematuhan pengguna dengan ISP. Rajah 2.2 menggambarkan model TPB asas.



Rajah 2.2 : Teori Perancangan Yang Di Rancang

2.4.3 Justifikasi Teori Yang Dipilih

Kebanyakan kajian terdahulu menumpukan kepada tingkah laku terhadap keselamatan maklumat di kalangan pekerja dalam organisasi; Walau bagaimanapun, untuk pengetahuan terbaik penyelidik, hanya sedikit yang dilakukan untuk menilai tingkah laku pematuhan keselamatan maklumat di kalangan pekerja (Gathan Narayana Samy et

al. 2009) sementara tidak ada kajian yang menyiasat pengantaraan kesan kesedaran keselamatan maklumat, terutamanya berkenaan dengan hubungan antara sokongan pengurusan dan tingkah laku pematuhan pekerja terhadap ISP.

Selain itu, kajian tentang faktor manusia seperti halangan keselamatan yang berkaitan dengan tingkah laku keselamatan maklumat tidak banyak diterokai. Oleh itu, kajian semasa bertujuan untuk mengadaptasi dua teori - TAM dan TPB - kerana kedua-dua teori ini terdiri daripada beberapa pembinaan yang banyak digunakan dalam pelbagai kajian untuk menjelaskan tingkah laku manusia. Oleh itu, objektif penyelidikan adalah untuk membangunkan model dengan menyesuaikan dua teori - TPB dan TAM - dan menamakannya sebagai Model Tahap Kesedaran Keselamatan Maklumat.

Semakin tinggi kesedaran pengguna tentang ancaman maklumat, semakin banyak kesedaran mereka terhadap ancamanya, sehingga menyebabkan pengurangan dalam insiden keselamatan. Adalah dipercayai bahawa apabila pengguna menyedari manfaat melaksanakan mekanisme perlindungan maklumat terhadap aset maklumat untuk mencegah ancaman yang melebihi kos menghapuskannya kemudian, mereka lebih cenderung untuk membuat langkah-langkah keselamatan yang betul, dan sebaliknya (Workman et al. 2008).

TAM dipilih kerana ia terdiri daripada beberapa bentuk yang tidak diwakili dalam penggunaan Sistem Maklumat (IS) dan teori-teori lain yang berkaitan, tetapi adalah penting untuk amalan keselamatan maklumat (Ng et al., 2009). Selain itu, TAM dapat mengukur atau meramalkan tingkah laku manusia dengan jayanya (Brown, Ottney & Nguyen 2011). Kajian ini memberi tumpuan kepada tingkah laku keselamatan pelindung pengguna akhir, yang ditakrifkan sebagai tingkah laku yang tidak melanggar dasar keselamatan organisasi.

Sementara itu, TPB dikenali sebagai model penting yang digunakan untuk menggambarkan kelakuan pengguna dalam penerapan teknologi maklumat (Fishbein & Ajzen 1975). Selain itu, TPB juga boleh menerangkan kelakuan kesadaran berasaskan

kognisi individu. Walau bagaimanapun, ia diperhatikan TPB mungkin tidak sesuai untuk memahami kelakuan biasa.

Menurut TPB, tingkah laku manusia dapat dimotivasi oleh apa yang orang lain fikir seseorang patut lakukan (Sun et al. 2006; Ajzen, 1991). Dengan ini, kajian ini menekankan tingkah laku pemimpin dalam memotivasi pengikut mereka untuk mengamalkan tingkah laku keselamatan yang betul. (Huang et al. 2011).

Adalah penting bagi pengurusan untuk memberikan komitmen dan sokongan penuh kepada pekerja mereka sebagai pengguna akhir teknologi maklumat mengenai amalan terbaik untuk tingkah laku keselamatan maklumat. Penglibatan peringkat atasan sedemikian boleh mempengaruhi kesedaran pengguna mengenai keselamatan maklumat. Ini juga ditekankan oleh penulis dari kajian sebelumnya yang mendapati bahawa pengurusan memainkan peranan penting dalam menggalakkan tingkah laku pengguna positif terhadap penggunaan teknologi maklumat (Ng et al. 2009).

Pengurusan atasan mesti mempunyai pengetahuan yang pasti mengenai kepentingan keselamatan maklumat untuk mewujudkan persekitaran organisasi yang kondusif untuk mencapai matlamat keselamatan. Kajian telah mencadangkan bahawa jika majikan dapat menyediakan satu set garis panduan keselamatan yang jelas dan memantau pekerja mereka secara ketat, pematuhan keselamatan maklumat akan meningkat (Herath & Rao 2009a).

Antara sebab utama yang disebutkan untuk pelaksanaan ISP yang lemah dalam organisasi adalah kurangnya sokongan pengurusan yang sepatutnya, kekurangan kuasa, dan kurangnya pemahaman mengenai pentingnya keselamatan maklumat (Brady 2011). Adalah penting bahawa pengurusan atasan memainkan peranan mereka dengan baik untuk memastikan keberkesanan keselamatan teknologi makluat melalui tingkah laku kepimpinan mereka.

Di samping itu, sokongan pengurusan adalah sama penting bagi pelaksanaan ISP, peruntukan untuk latihan keselamatan maklumat yang mencukupi dan pelaksanaan

program kesedaran keselamatan yang berkesan untuk pekerja. Berdasarkan tinjauan, konsep TPB disesuaikan dengan meletakkan tingkah laku kepimpinan (SN), isyarat untuk tindakan, latihan keselamatan maklumat, serta pelaksanaan ISP (PBC) sebagai petunjuk tahap sokongan pengurusan.

2.5 FAKTOR KESEDARAN KESELAMATAN MAKLUMAT

Kesedaran keselamatan maklumat merangkumi tahap kefahaman para pekerja terhadap ancaman keselamatan maklumat yang boleh mempengaruhi proses organisasi dan juga pemahaman mereka terhadap kepentingan mematuhi tingkah laku keselamatan maklumat untuk mencegah ancaman keselamatan maklumat (Ahlan et al. 2011).

Ramai penyelidik berpendapat bahawa keberkesanan keselamatan maklumat boleh dicapai jika pekerja mengamalkan tingkah laku keselamatan maklumat yang mencukupi, mematuhi dasar dan prosedur keselamatan yang dilaksanakan di dalam organisasi (Li, Zhang & Sarathy 2010; Safa et al. 2016; Warkentin et al. 2011).

Para pekerja harus sedar mengenai kebarangkalian ancaman keselamatan maklumat yang mungkin wujud di dalam organisasi dan akibat daripada ancaman keselamatan maklumat kepada para pekerja dan organisasi jika ada ancaman (Mejias 2012). Para pekerja mesti dapat mengenal pasti ancaman keselamatan maklumat (Thomson et al. 2006) supaya mereka dapat menyesuaikan tindakan mereka. Walau bagaimanapun, tindakan ini adalah berdasarkan kepada keputusan mereka, dan para pekerja biasanya membuat keputusan berdasarkan pemahaman mereka terhadap subjek tersebut (Kruger & Kearney 2006).

2.5.1 Faktor Sikap

Sikap adalah perasaan umum atau pendapat seseorang mengenai sesuatu (Oladosu 2012). Ia adalah pengawal tingkah laku sebenar seseorang secara sedar atau tidak secara

sedar. Sikap adalah sebahagian daripada struktur kognitif yang digunakan oleh penjawat awam untuk mengatur, menstrategikan pengalaman dan tingkah laku mereka.

Sikap merupakan respon atau reaksi yang masih tertutup dari seseorang terhadap sesuatu perkara. Ianya merupakan kesediaan untuk bertindak dan bukan merupakan pelaksanaan motif tertentu. Menurut Hu et al. (2012), sikap dipengaruhi oleh beberapa faktor seperti pengalaman peribadi, kebudayaan, pengaruh orang lain yang dianggap penting, media massa serta faktor emosi dalaman seseorang individu. Oleh kerana sikap merupakan sesuatu yang difikir di dalam fikiran individu maka ianya sukar dilihat oleh orang lain dengan segera.

Sikap penjawat awam terhadap kesedaran dalam keselamatan maklumat adalah berkenaan penerimaan atau penolakan mengaplikasikan keselamatan maklumat di persekitaran tempat kerja. Cheng et al. (2013) menjelaskan bahawa penjawat awam menunjukkan minat dan motivasi yang tinggi ke arah mempelajari teknologi maklumat dan komunikasi namun tidak berminat untuk mengekalkan tahap keselamatannya. Ia juga berpendapat bahawa penjawat awam mempunyai sikap konstruktivisme dan kepercayaan tradisional mengenai pembelajaran teknologi maklumat dan komunikasi.

Penjawat awam yang bersikap konstruktivis adalah pengguna komputer yang sangat aktif manakala penjawat awam dengan kepercayaan tradisional kurang berkemampuan menggunakan komputer dan teknologi maklumat dan komunikasi (Metalidou et al. 2014). Di samping itu, pihak pengurusan harus menyemai tingkah laku keselamatan yang baik di kalangan pekerja dan menjadikan kesedaran keselamatan maklumat sebagai satu keutamaan di dalam pembangunan ISP (Shropshire et al. 2015).

Melalui latihan dan pendidikan yang berkesan, sikap dan kemahiran keselamatan maklumat para pekerja boleh diperbaiki kerana para pekerja digalakkan untuk mempunyai amalan keselamatan maklumat yang baik seperti yang disyorkan oleh organisasi mereka (Rezgui & Marks 2008). Sementara itu, penulis kajian lain berpendapat bahawa program atau kempen kesedaran keselamatan mempengaruhi

tingkah laku atau sikap bagi pematuhan pekerja terhadap keselamatan maklumat (Albrechtsen & Hovden 2010; Eminağaoğlu et al. 2009; Yoshikai et al. 2011).

Walaupun pihak pengurusan memberi sokongan penuh kepada keselamatan maklumat dengan menganjurkan latihan keselamatan dan melaksanakan teknologi keselamatan canggih tetapi jika para pekerja masih tidak menyedari dan tidak peduli tentang pentingnya mengamalkan tingkah laku keselamatan maklumat, objektif keselamatan tidak akan tercapai (Aloul 2012). Menurut Hu et al. (2012), perlu juga diambil kira bahawa kesedaran keselamatan maklumat boleh memeterai hubungan di antara sokongan pengurusan dengan tingkah laku pematuhan para pekerja terhadap ISP.

2.5.2 Faktor Sokongan Pihak Pengurusan

Sokongan penuh daripada pihak pengurusan di dalam mana-mana organisasi adalah penting kerana ia dapat memastikan keberkesanan sistem keselamatan maklumat dan boleh menghasilkan persekitaran yang selamat untuk pengendalian maklumat (Safa et al. 2015; Hu et al. 2012; Brady 2011).

Sokongan pihak pengurusan merujuk kepada komitmen daripada pihak pengurusan di dalam organisasi seperti yang dilihat oleh pekerja (Al-Salihy et al. 2003). Walau bagaimanapun, sokongan pihak pengurusan masih di peringkat awal di dalam kajian keselamatan maklumat dengan kebanyakan kajian terdahulu yang lebih fokus kepada teknologi keselamatan (Brady 2011; Santos et al. 2008).

Seperti yang telah dibincangkan sebelum ini, pihak pengurusan dapat menunjukkan sokongan mereka terhadap tingkah laku keselamatan maklumat melalui penganjuran dan membangunkan latihan keselamatan maklumat, program kesedaran dan pelaksanaan ISP. Latihan keselamatan maklumat, program kesedaran dan pelaksanaan ISP adalah kaedah untuk memaklumkan kepada pekerja tentang ISP organisasi (Martin & Rice 2011), yang bertujuan untuk memperkenalkan dan menyediakan maklumat mengenai pentingnya penggunaan langkah balas/tindakan balas

keselamatan untuk mengelakkan maklumat ancaman keselamatan dan kesan ancaman kepada organisasi.

Para pemimpin di dalam sesebuah organisasi perlu menunjukkan tingkah laku keselamatan yang positif dan menggalakkan pekerja mereka untuk menghadiri mana-mana latihan keselamatan maklumat dan mewajibkan para pekerja mereka untuk mematuhi dasar dan peraturan keselamatan yang dilaksanakan di dalam organisasi (Safa et al. 2015). Menurut Ahlan et al. (2011), kemahiran kepimpinan adalah penting di dalam mewujudkan asas untuk kesedaran keselamatan dan telah dikatakan bahawa kepimpinan mempunyai kesan terhadap kesedaran para pekerja mengenai pentingnya mematuhi ISP organisasi.

Tingkah laku para pekerja di dalam organisasi kebanyakannya dipengaruhi oleh pihak atasan mereka seperti pengarah, pengurus dan penyelia yang menjadi pemimpin di dalam sesebuah organisasi. Ini disokong oleh penyelidikan lain yang juga mendapati bahawa tingkah laku pihak atasan juga mempunyai kesan yang signifikan ke atas niat para pekerja untuk mematuhi ISP organisasi (Hagen Merete, Albrechtsen & Hovden 2008; Ifinedo 2014; Kyobe 2010; Wiant 2005) .

Selain itu, Kreicberga (2010) menyatakan bahawa pengetahuan pekerja dan pengalaman mereka juga dapat dibangunkan berdasarkan kelakuan pengurusan atasan mereka dan rakan sekerja yang lain. Oleh itu, pihak pengurusan mesti memberi sokongan penuh dan membina persekitaran positif di dalam organisasi untuk memastikan semua pekerja mematuhi peraturan dan undang-undang organisasi menerusi program kesedaran keselamatan maklumat.

2.5.3 Faktor Latihan Dan Pendidikan

Latihan dan pendidikan dasar keselamatan maklumat adalah program yang bertujuan untuk memperkenalkan dan menyediakan maklumat mengenai kepentingan sistem keselamatan, yang mana semua pekerja harus mematuhinya. Kesedaran keselamatan maklumat boleh dicapai melalui latihan keselamatan pekerja kerana latihan adalah salah

satu cara untuk menyampaikan ISP organisasi (Siponen et al. 2014).

Latihan keselamatan yang terurus dengan baik boleh mendidik para pekerja untuk mematuhi ISP (Kim 2014). Oleh itu, pihak pengurusan mesti memastikan bahawa organisasi mereka telah melaksanakan latihan keselamatan dengan berkesan.

Penulis kajian terdahulu juga menyatakan bahawa pekerja yang menerima latihan keselamatan menunjukkan kelakuan yang lebih meyakinkan dan lebih cenderung untuk mematuhi ISP organisasi (Ifinedo 2014). Hu et al. (2012) menyatakan bahawa pihak pengurusan boleh membuat perubahan berkenaan dengan tingkah laku keselamatan. Ini boleh dilakukan dengan membina budaya keselamatan di dalam organisasi (Da Veiga & Martins 2015).

Selain itu, latihan keselamatan maklumat juga dapat meningkatkan kemahiran pekerja untuk menggunakan sistem keselamatan dengan betul yang dapat mencegah ancaman keselamatan (Beas & Salanova 2006; Liang & Xue 2009; Torkzadeh & Van Dyke 2002). Program latihan atau kempen kesedaran keselamatan telah dilaporkan sebagai cara terbaik untuk meningkatkan kesedaran para pekerja kerana mesej keselamatan dapat mencapai para pekerja dengan lebih efisien (Rezgui & Marks 2008).

Pelaksanaan latihan keselamatan maklumat dan program kesedaran keselamatan adalah tanggungjawab pihak pengurusan. Pihak pengurusan harus mempertimbangkan dan memberi sokongan sepenuhnya kepada isu ini bagi memastikan tingkah laku keselamatan para pekerja boleh diterima. Kandungan latihan keselamatan maklumat dan program kesedaran keselamatan harus merangkumi maklumat terperinci termasuklah tahap kerosakkan jika ancaman keselamatan ini tersebar di dalam sesebuah organisasi (Siponen et al. 2014).

Oleh itu, pihak pengurusan harus menjalankan latihan keselamatan maklumat untuk semua pekerja di dalam organisasi. Latihan adalah alat yang berkesan untuk memastikan pengguna mempunyai sikap yang tepat terhadap keselamatan maklumat dan seterusnya dapat mengurangkan bilangan insiden keselamatan (Al-Omari & El-Gayar 2012; Jenkins et al. 2012) . Menurut Eminağaoğlu et al. (2009), latihan

keselamatan adalah mekanisme yang berkesan untuk mengurangkan risiko keselamatan maklumat.

Walau bagaimanapun, latihan keselamatan harus dijalankan secara kerap kerana manusia cenderung lupa apa yang mereka pelajari. Oleh itu, adalah penting bagi pihak organisasi untuk menjalankan latihan keselamatan yang berterusan bagi memastikan para pekerja sentiasa mengetahui tentang pentingnya keselamatan maklumat (Hagen Merete et al. 2008).

Selain itu, latihan keselamatan yang sesuai untuk para pekerja adalah penting kerana ia dapat mewujud dan mengekalkan kesedaran keselamatan maklumat yang tinggi (Ifinedo 2014; Puhakainen 2006). Oleh itu, latihan keselamatan yang efektif seharusnya dapat menyampaikan mesej tentang risiko keselamatan maklumat kepada semua pekerja dan menunjuk ajar mereka bagaimana untuk menggunakan amalan keselamatan IS dengan betul.

Latihan keselamatan maklumat juga dapat mengatasi masalah kesedaran keselamatan maklumat kerana telah dilaporkan bahawa latihan keselamatan maklumat merupakan salah satu mekanisme keselamatan yang dapat mempengaruhi kesedaran keselamatan maklumat oleh para pekerja (Hagen Merete et al. 2008; Jenkins et al. 2012).

2.5.4 Faktor Polisi/Dasar Keselamatan Maklumat

Adalah penting bagi organisasi menyediakan dokumentasi ISP yang betul supaya para pekerja dapat memahami dan mengamalkannya. Kajian semasa menunjukkan bahawa ISP yang didokumentasi dengan baik dengan penerangan yang jelas dapat meningkatkan kesedaran pengguna tentang keselamatan maklumat (Al-Omari et al. 2013).

Dengan itu, insiden keselamatan di dalam organisasi dapat dikurangkan. Kajian terdahulu menegaskan bahawa ISP adalah penting kerana ia menyediakan satu set

peraturan dan prosedur yang membantu menentukan tahap keselamatan maklumat yang disyorkan di dalam organisasi yang harus diikuti oleh para pekerja (Yildirim Y. et al. 2011).

Secara umumnya, Safa et al. (2016) menyatakan bahawa ISP adalah pernyataan niat dan objektif dasar syarikat yang bertujuan a) Untuk menunjukkan lembaga dan pengurusan kanan syarikat komitmen terhadap keselamatan maklumat. b) Untuk menetapkan arahan untuk pelaksanaan dan menekankan bahawa mereka melihatnya sebagai bahagian penting dari operasi harian syarikat c) Untuk mengekalkan kesinambungan operasi dan seterusnya meneruskan untuk menyediakan perkhidmatan d) Untuk melindungi aset syarikat.

ISP ini juga menekankan kepentingan aspek keselamatan maklumat seperti bagaimana hendak melindungi maklumat berharga (Knapp et al. 2009) dan membantu mengurangkan bilangan kejadian keselamatan di dalam organisasi (Kruger & Kearney 2006). Walau bagaimanapun, insiden keselamatan tidak dapat dikurangkan jika tingkah laku keselamatan maklumat di kalangan pekerja tidak dapat ditingkatkan, terutama jika mereka tidak mengetahui adanya ISP.

ISP tidak dapat dilaksanakan dengan berkesan jika para pekerja tidak mengetahui tentangnya. Oleh itu, ISP perlu digunakan dan diedarkan dengan betul dan tepat di seluruh organisasi dan diperkenalkan kepada semua pekerja (Höne & Eloff 2002). Menurut Höne & Eloff (2002), pengedaran ISP boleh dilakukan semasa latihan keselamatan maklumat dengan menggunakan salinan berasaskan kertas atau salinan dokumen elektronik, melalui penerbitan dokumen di laman web dalaman.

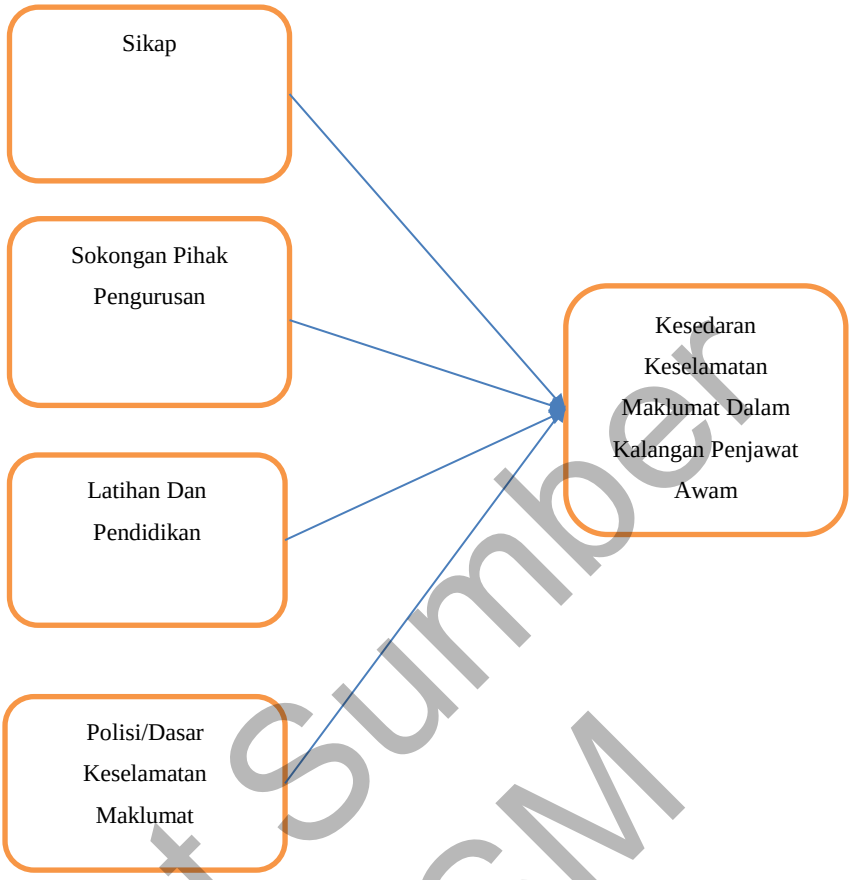
Di samping itu, pihak pengurusan harus memastikan bahawa kandungan ISP semasa program latihan dan kesedaran jelas menggariskan tanggungjawab para pekerja, menentukan penggunaan sistem yang dibenarkan dan yang tidak dibenarkan, prosedur untuk melaporkan sebarang ancaman yang disyaki akan terjadi kepada sistem, menentukan penalti bagi pelanggaran peraturan dan menyediakan mekanisme untuk mengemaskini ISP (Whitman 2004).

Jika dasar keselamatan maklumat mudah difahami, dapat diterima dengan mudah dan tidak terlalu tegas, ia akan meningkatkan kesedaran pengguna dan dengan demikian, akan mendorong pengguna untuk bertingkahlaku bersesesuaian dengan keselamatan maklumat. Gunson et al. (2011) berpendapat bahawa jika proses keselamatan sukar digunakan, pengguna akan menghindarinya dan akan gagal menggunakannya dengan betul. Sebagai contoh, untuk membuat kata laluan yang sangat selamat, beberapa aksara dan nombor teks perlu digabungkan, yang menjadikannya sukar bagi pengguna untuk mengingati kata laluan.

2.6 MODEL KONSEPTUAL

Berdasarkan kajian literasi yang telah dilakukan, beberapa faktor kesedaran keselamatan maklumat dalam kalangan pekerja telah dikenalpasti. Terdapat empat (4) faktor kesedaran keselamatan maklumat dalam kalangan pekerja iaitu sikap, sokongan pihak pengurusan, latihan dan Pendidikan dan polisi/dasar keselamatan maklumat.

Rajah 2.3 menunjukkan model konseptual yang menggambarkan faktor kesedaran keselamatan maklumat dalam kalangan pekerja. Faktor ini diperolehi berdasarkan ulasan kesusasteraan yang dilakukan dan digunakan pada bahagian kaji selidik untuk membina soalan.



Rajah 2.3 Model Konseptual

2.7 KESIMPULAN

Berdasarkan kajian kesusasteraan yang dilaksanakan, didapati bahawa faktor sikap, sokongan pihak pengurusan, polisi/dasar keselamatan maklumat dan latihan/pendidikan merupakan faktor yang penting bagi memastikan penjawat awam mempunyai kesedaran keselamatan maklumat yang tinggi. Kesedaran keselamatan maklumat dalam kalangan penjawat awam perlulah dinilai dan ditambah baik secara berterusan bagi memastikan sistem penyampaian kerajaan terjamin dan dapat memenuhi keperluan pengguna.

Kajian ini akan menggunakan model konseptual yang telah dikenalpasti sebagai asas model awal kajian dan juga asas penghasilan instrumen awal kajian. Model awal

kajian yang dihasilkan akan diuji secara empirikal bagi membolehkan persoalan kajian yang digariskan dalam Bab I dapat dijawab.

BAB III

METODOLOGI KAJIAN

3.1 PENGENALAN

Metodologi kajian yang lengkap dan komprehensif adalah penting bagi memastikan objektif kajian dapat dipenuhi seterusnya dapat menjawab persoalan kajian yang telah digariskan. Metodologi kajian yang berkesan bukan hanya mampu menjawab persoalan kajian secara empirikal dan juga analitikal malah dapat menyumbang kepada teori dan praktikal bidang kajian. Pemilihan metodologi kajian perlulah mengambil kira objektif, persoalan kajian dan juga konteks kajian dijalankan.

Bagi tujuan kajian ini, pendekatan secara kuantitatif dan kualitatif telah dipilih untuk dilaksanakan. Dengan gabungan pendekatan ini diharapkan persoalan kajian dapat dijawab dengan tepat dan seterusnya membolehkan analisa mendalam dibuat bagi setiap dimensi yang dikaji.

Penerangan seterusnya merangkumi perincian empat (4) fasa pendekatan kajian iaitu penghasilan model konseptual, penghasilan instrumen awal, pengesahan instrumen kajian dan pengesahan model serta kesimpulan yang merumuskan keseluruhan bab.

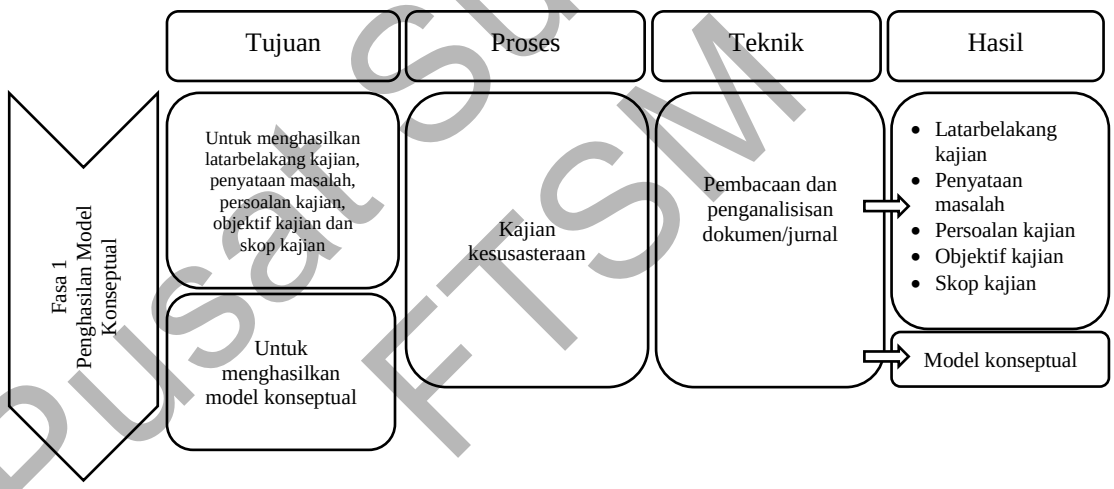
3.2 PENDEKATAN KAJIAN

Pendekatan kajian distrukturkan kepada empat (4) fasa utama iaitu penghasilan model konseptual, penghasilan instrumen awal, pengesahan instrumen kajian dan pengesahan model. Setiap fasa diperincikan kepada proses-proses yang terlibat, tujuan pelaksanaan setiap proses, teknik yang digunakan bagi setiap proses dan hasil akhir bagi setiap

proses. Gambaran pendekatan kajian adalah seperti yang ditunjukkan dalam Rajah 1.3 dalam Bab I.

3.3 FASA 1: PENGHASILAN MODEL AWAL

Penghasilan model awal kajian dilaksanakan melalui kajian kesusasteraan dengan pembacaan dan penganalisisan secara sistematik ke atas jurnal-jurnal yang berkaitan dengan bidang kesedaran keselamatan maklumat. Kajian kesusasteraan yang komprehensif membolehkan pemahaman yang lebih mendalam berkaitan subjek kajian dan seterusnya mampu menjawab persoalan kajian dengan lebih tepat dan terperinci. Proses penghasilan model konseptual adalah seperti Rajah 3.1.



Rajah 3.1 Proses penghasilan model konseptual

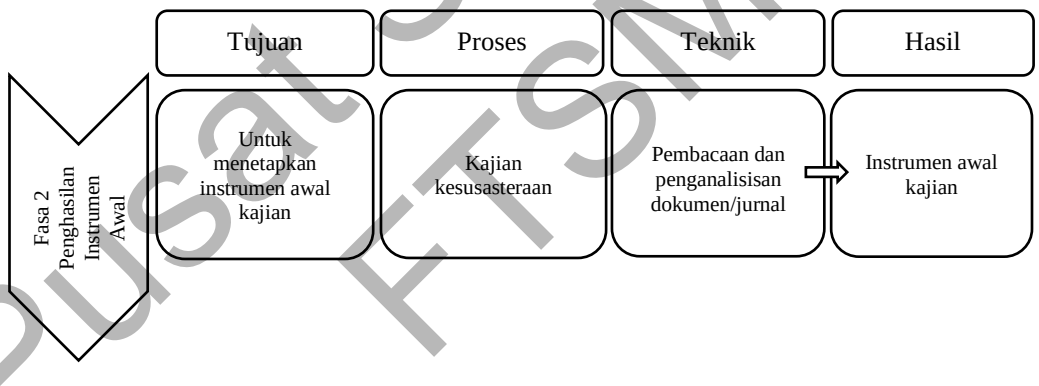
Bagi penghasilan model konseptual, kajian kesusasteraan dilaksanakan yang bertujuan untuk memahami dengan lebih mendalam bidang yang dikaji melalui penghasilan latar belakang kajian, permasalahan kajian, objektif kajian, persoalan kajian dan skop kajian.

Ini melibatkan penghasilan latar belakang kajian, permasalahan kajian, objektif kajian, persoalan kajian dan skop kajian telah dibincangkan dengan lanjut dalam Bab I

dan Bab II sebelum ini. Hasil kajian ini membantu dalam mengenalpasti bidang yang hendak dikaji, trend semasa kajian dan seterusnya mengenal pasti jurang yang wujud dan apakah yang sepatutnya dicapai oleh kajian ini. Peringkat ini penting dalam memberi kefahaman mengenai bidang kajian dan menjadi panduan penyelidikan.

3.4 FASA 2: PENGHASILAN INSTRUMEN AWAL

Fasa seterusnya melibatkan penghasilan instrumen awal kajian yang dilaksanakan melalui kajian kesusasteraan ke atas jurnal-jurnal berkaitan tahap kesedaran keselamatan maklumat. Instrumen awal kajian yang dihasilkan melalui fasa ini akan digunakan dalam proses kajian sebenar bagi tujuan pengumpulan data. Proses penghasilan instrumen awal adalah seperti Rajah 3.2.



Rajah 3.2 Proses penghasilan instrumen awal

Bagi tujuan kajian ini, instrumen kajian diadaptasi daripada kajian-kajian terdahulu yang telah diuji secara empirikal. Dalam bidang sistem maklumat, terdapat banyak kajian yang dijalankan dan secara tidak langsung menyediakan banyak pilihan instrumen kualitatif dan kuantitatif yang telah disahkan untuk diguna pakai (Kock & Verville 2012).

Kajian ini telah mengadaptasi instrumen kaji selidik berdasarkan kepada kajian (Kaur & Mustafa 2013) dan juga (Rounds et al. 2008). Instrumen kajian yang digunakan adalah selaras dengan model awal yang dihasilkan dalam fasa sebelum ini. Ini bagi memastikan instrumen yang digunakan dapat menjawab kedua-dua per soalan kajian yang telah digariskan. Instrumen kaji selidik yang dihasilkan terbahagi kepada tiga (3) bahagian utama iaitu:

a) Bahagian A- Demografi responden
b) Bahagian B- Dimensi kesedaran keselamatan maklumat
c) Bahagian C- Cadangan

Bahagian A terdiri daripada tujuh (7) soalan berkaitan demografi responden yang diukur menggunakan skala nominal. Manakala bahagian B terdiri daripada 25 item yang diukur menggunakan skala Likert. Pengukuran bagi skala Likert bermula daripada satu (1) hingga tujuh (5) (sangat tidak setuju sehingga sangat setuju).). Bahagian B diadaptasi daripada kajian (Kaur & Mustafa 2013) dan juga (Rounds et al. 2008). Bahagian C adalah ruang cadangan yang boleh diisi oleh responden yang dapat menyokong soal selidik ini.

Ringkasan instrumen kaji selidik adalah seperti di Jadual 3.1. Berdasarkan penilaian pakar, instrumen kajian telah dikemas kini secara terperinci daripada segi kandungan dan juga format sebelum digunakan dalam kajian sebenar seperti di Jadual 3.2. Penambahbaikan instrumen kajian yang telah diputuskan adalah seperti berikut:

d) Sebanyak tigabelas (13) item telah dihapuskan. Menjadikan jumlah item yang disahkan untuk digunakan dalam kajian sebenar adalah sebanyak 33 item yang terdiri daripada tujuh (7) item di bahagian A, dua puluh lima (25) item di bahagian B dan satu (1) item di bahagian C. Kebanyakan item yang dihapuskan ialah kerana mempunyai maksud yang hampir sama dengan item lain yang berada di dalam dimensi yang sama. Selain daripada itu, item juga dihapuskan kerana boleh mengelirukan responden apabila diinterpretasikan dalam konteks kajian.

e) Beberapa frasa dimensi dan item telah dikemas kini bagi memantapkan lagi semantik ayat bagi memudahkan pemahaman pengguna dalam konteks kajian.

f) Pakar juga turut mencadangkan agar instrumen dihasilkan dalam satu bahasa sahaja iaitu Bahasa Malaysia bagi mengelakkan kekeliruan apabila mengisi kaji selidik. Ini kerana terjemahan yang telah dibuat lebih mudah difahami dan mengambil kira maksud sebenar dalam konteks Bahasa Malaysia.

Instrumen kaji selidik hasil penilaian kesemua pakar adalah seperti di Lampiran B. Instrumen yang diadaptasi telah diterjemahkan ke dalam Bahasa Malaysia. Semua item adalah wajib dijawab oleh responden kecuali di Bahagian C. Instrumen kaji selidik yang telah digunakan untuk edaran kepada responden adalah seperti di Lampiran C.

Jadual 3.1 Ringkasan instrumen kaji selidik selepas penilaian pakar

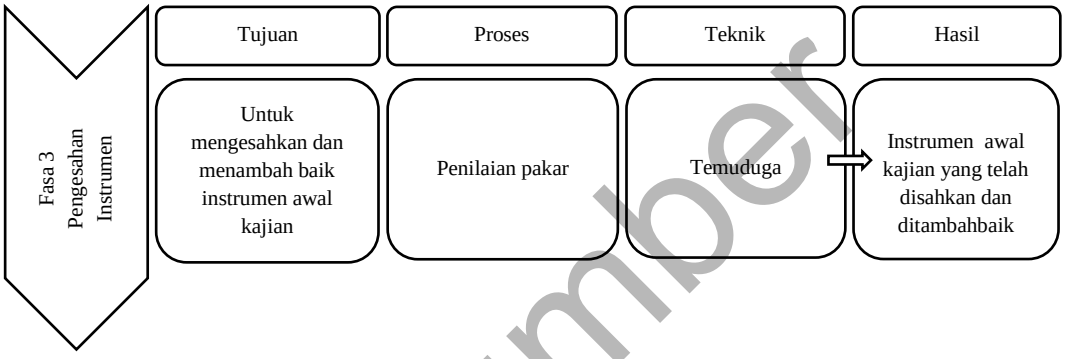
Bahagian/ Kod	**Dimensi**	**Bil. Item Sebelum Penilaian Pakar**	**Bil. Item Selepas Penilaian Pakar**	**Kod Item Dihapus**	**Bil. Item Dihapus**
Bahagian A					
1 hingaa 7	Demografi	9	7	1, 2	2
Bahagian B					
A1 hingga A8	Sikap	8	5	A6, A7, A8	3
B1 hingga B7	Sokongan Pihak Pengurusan	7	5	B5, B6	2
C1 hingga C7	Latihan dan Pendidikan	7	5	C6, C7	2
D1 hingga D7	Polisi dan Dasar Keselamatan Maklumat	7	5	D1, D7	2
E1 hingga E7	Kesedaran Keselamatan Maklumat	7	5	E1, E2	2
Bahagian C					
	Cadangan	1	1	Tiada	1

Jadual 3.2 Ringkasan instrumen awal kaji selidik

Bahagian/ Kod	Faktor/Dimensi	Pengukuran Konstruk	Bil. Item
Bahagian A 1 hingga 7	**Demografi**	Maklumat Umum Pengguna	7
Bahagian B		**Faktor kesedaran keselamatan maklumat**	
A1 hingga A5	Sikap	Sejauh manakah sikap berhubungkait dengan kesedaran keselamatan maklumat	5
B1 hingga B5	Sokongan Pihak Pengurusan	Sejauh manakah sokongan pihak pengurusan membantu mempertingkatkan tahap kesedaran keselamatan maklumat	5
C1 hingga C5	Latihan dan Pendidikan	Sejauh manakah latihan/pendidikan membantu menambah kefahaman berkaitan isu keselamatan maklumat	5
		bersambung...	
...sambungan D1 hingga D5	Polisi/ Dasar Keselamatan Maklumat	Sejauh manakah polisi / dasar membantu meningkatkan kesedaran keselamatan maklumat	5
E1 hingga E5	Kesedaran Keselamatan Maklumat	Sejauh manakah tahap kesedaran keselamatan maklumat dalam kalangan pengguna	5
Bahagian C	Cadangan	Cadangan penambahbaikan kesedaran keselamatan maklumat dalam kalangan pengguna	1

3.5 FASA 3: PENGESAHAN INSTRUMEN KAJIAN

Fasa ketiga melibatkan proses pengesahan instrumen kajian yang telah dihasilkan dalam fasa kedua. Proses pengesahan instrumen adalah seperti Rajah 3.4.



Rajah 3.4 Proses pengesahan instrumen kajian

Pengesahan instrumen dilaksanakan secara penilaian pakar menggunakan kaedah temuduga. Proses pengesahan bertujuan memastikan item yang terkandung di dalam instrumen yang dicadangkan adalah meliputi semua dimensi keselamatan maklumat, tiada pertindihan antara satu sama lain dan seterusnya boleh difahami dengan mudah.

Selain daripada itu, penilaian pakar turut memastikan instrumen dibentuk menggunakan bahasa yang baik dan boleh difahami dengan jelas seterusnya menghasilkan item berkualiti dan menepati matlamat kajian. Walaupun instrumen diadaptasi daripada kajian sebelumnya di mana kesahihan dan kebolehpercayaan item telah dibuktikan secara empirikal, penilaian pakar masih perlu dibuat bagi memastikan kesesuaiannya dalam konteks kajian semasa.

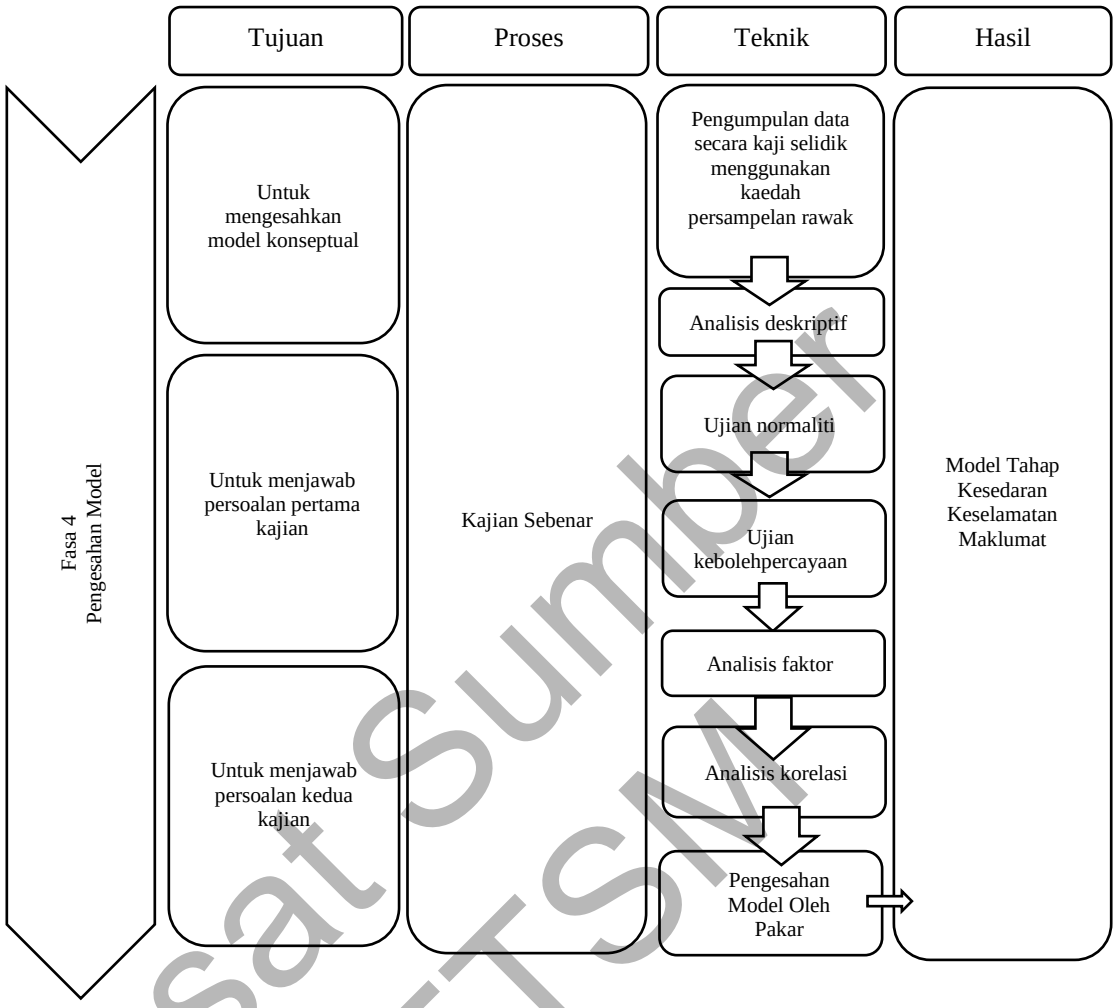
Pengesahan instrumen dilaksanakan secara temu bual secara individu. Hasil akhir fasa ini merupakan instrumen kaji selidik yang telah ditambahbaik dan sedia untuk digunakan dalam kajian sebenar. Aktiviti-aktiviti yang terlibat dalam fasa ini termasuklah pemilihan pakar, pengesahan instrumen dan penambahbaikan instrumen.

3.6 FASA 4: PENGESAHAN MODEL AWAL

Fasa keempat merupakan fasa pengesahan model konseptual yang telah dicadangkan berdasarkan kajian lepas. Selain daripada mengesahkan model konseptual, fasa ini juga akan turut menjawab kedua-dua persoalan kajian yang telah digariskan.

Pengesahan model konseptual dilaksanakan secara analisis statistik menggunakan data yang dikumpulkan daripada responden yang terpilih. Pengumpulan data dibuat menggunakan instrumen kaji selidik yang telah disahkan dan ditambah baik dalam fasa ketiga sebelum ini. Analisis statistik dibuat menggunakan perisian *Statistical Package for the Social Sciences* (SPSS). Hasil akhir fasa ini merupakan model tahap kesedaran keselamatan maklumat berdasarkan analisis data yang dibuat. Proses pengesahan model konseptual adalah seperti di Rajah 3.5.

Pelaksanaan kaji selidik melibatkan aktiviti seperti pensampelan, penyediaan dan pengagihan instrumen kajian dan pengumpulan dan persediaan data. Manakala analisis data melibatkan analisis deskriptif, pengukuran normaliti data, ujian kebolehpercayaan, analisis faktor dan analisis korelasi serta pengesahan model oleh pakar.



Rajah 3.5 Proses pengesahan model konseptual

3.6.1 Analisis Data

Data yang telah dikumpulkan melalui kaji selidik dianalisis secara terperinci menggunakan perisian SPSS. Analisis data terbahagi kepada lima (5) bahagian iaitu, analisis deskriptif, pengukuran normaliti data, ujian kebolehpercayaan, analisis faktor dan analisis korelasi. Perincian bagi analisis data diterangkan dalam bahagian berikut.

a) Analisis deskriptif

Analisis deskriptif dilaksanakan untuk menghuraikan ciri-ciri sampel yang dikaji. Bagi maklumat umum responden, huraian dibuat daripada segi peratusan. Manakala bagi faktor kesedaran keselamatan maklumat, huraian melibatkan maklumat min, median dan mod. Analisis deskriptif yang dijalankan dapat memberi gambaran awal secara menyeluruh corak data yang diperolehi.

b) Pengukuran normaliti data

Pengukuran normaliti data dibuat bagi memastikan sama ada data yang dikumpul tertabur secara normal atau sebaliknya. Semakan bentuk taburan data adalah penting dalam menentukan ujian statistik yang boleh dilaksanakan. Ujian dibuat dengan mengukur nilai *skewness* dan nilai *kurtosis* ke atas data.

c) Ujian kebolehpercayaan

Ujian kebolehpercayaan dilaksanakan untuk menilai konsistensi dalaman item berdasarkan darjah korelasi di antara setiap item dalam mengukur dimensi yang sama. Ujian kebolehpercayaan juga dapat menentukan nilai ralat rawak yang mungkin wujud dalam pengukuran (Nunnally, & Bernstein 1994).

Tahap kebolehpercayaan item diukur menggunakan nilai *Cronbach's coefficient alpha* (CA) yang dibangunkan oleh (Cronbach 1951). Nilai CA dinyatakan dalam julat 0 hingga 1. Interpretasi nilai CA dikelaskan kepada enam (6) kategori iaitu, melebihi 0.9 (cemerlang), melebihi 0.8 (baik), melebihi 0.7 (boleh diterima), melebihi 0.6 (diragui), melebihi 0.5 (lemah) dan kurang daripada 0.5 (tidak boleh diterima) (George, & Mallery 2003). Nilai CA 0.7 ditetapkan sebagai nilai minimum kebolehpercayaan (DeVellis 2003; Lee et al. 2002; Nunnally 1978).

d) Analisis faktor

Analisis faktor merupakan salah satu teknik statistik yang digunakan untuk mengenal pasti dan memahami struktur hubung kait item bagi setiap dimensi (Gorsuch 1983; Kim & Mueller 1978). Walaupun ujian kebolehpercayaan menunjukkan wujud hubung kait atau konsistensi yang tinggi antara item di bawah dimensi yang sama, namun analisis faktor masih perlu dilaksanakan kerana kemungkinan wujud lebih daripada satu dimensi bagi item yang dikelompokkan di bawah dimensi yang sama (Gliem & Gliem 2003).

Melalui analisis faktor, pengenalpastian dibuat sama ada sesuatu item berada di bawah kelompok dimensi yang sama atau berlainan berdasarkan nilai faktor muatan (*loading factor*) bagi setiap item. Secara teorinya, item-item yang memperolehi nilai faktor muatan yang jelas dan kuat perlu dikekalkan dalam komponen atau dimensi yang sama, manakala item-item yang memperolehi nilai faktor muatan yang rendah perlu diletakkan di dalam komponen atau dimensi yang berlainan (Matsunaga 2010) ataupun dipertimbangkan untuk dihapuskan.

Walau bagaimanapun, tiada kaedah yang jelas bagi menetapkan nilai faktor muatan dalam mengekalkan item di dalam sesuatu komponen atau dimensi (Comrey & Lee 1992; Gorsuch 1983) dan kerap memerlukan penilaian tambahan oleh pengkaji (Matsunaga 2010).

e) Analisis korelasi

Analisis korelasi bertujuan untuk menguji dan menerangkan arah serta kekuatan hubungan linear bagi setiap dimensi yang dikaji menggunakan teknik *Pearson* yang direka untuk data berformat skala.

Arah hubungan diterangkan dengan tanda positif atau negatif bagi setiap nilai korelasi. Arah positif (+) bermaksud peningkatan pada satu dimensi memberi kesan kepada peningkatan dimensi yang lain dan sebaliknya.

Manakala arah negatif (-) bermaksud peningkatan pada satu dimensi mengurangkan dimensi yang lain dan sebaliknya.

Kekuatan hubungan pula diterangkan berdasarkan nilai korelasi yang terhasil. Kekuatan hubungan bagi nilai korelasi diklasifikasikan kepada tiga (3) kategori bagi memudahkan interpretasi iaitu kekuatan hubungan lemah (nilai r=.10 hingga .29), kekuatan hubungan sederhana (nilai r=.30 hingga .49) dan kekuatan hubungan kuat (r=.5 hingga 1.0) (Cohen 1988).

Nilai korelasi sama ada +1 atau -1 menunjukkan dimensi mempunyai korelasi sempurna di mana nilai pada satu dimensi boleh ditentukan dengan tepat apabila mengetahui nilai dimensi yang lain. Manakala nilai korelasi 0, menunjukkan tiada perhubungan antara dimensi tersebut.

Analisis korelasi mampu menjawab persoalan kajian yang pertama iaitu adakah wujud hubungan antara dimensi keselamatan maklumat dengan dimensi kesedaran keselamatan maklumat. Hasil akhir analisis korelasi merupakan model akhir kesedaran keselamatan maklumat yang telah disahkan.

3.7 KESIMPULAN

Bab ini menerangkan secara terperinci pendekatan kajian yang terdiri daripada empat (4) fasa iaitu penghasilan model konseptual, penghasilan instrumen awal kajian, pengesahan instrumen kajian dan pengesahan model. Pendekatan kajian yang digunakan bertujuan untuk mencapai objektif kajian seterusnya berupaya menjawab persoalan kajian yang telah ditetapkan dalam Bab I.

BAB IV

HASIL PENGUJIAN DAN PERBINCANGAN

4.1 PENGENALAN

Pengujian dan perbincangan hasil kajian adalah berdasarkan data yang diperolehi melalui kaji selidik yang telah dijalankan. Kaji selidik yang dilaksanakan menggunakan instrumen yang telah disahkan melalui proses penilaian pakar. Kaji selidik telah diedarkan menggunakan perkhidmatan atas talian *Google Survey* dan edaran secara manual. Seterusnya, data telah diproses menggunakan perisian SPSS.

Analisis data yang dilaksanakan melibatkan analisis deskriptif, pengukuran normaliti data, ujian kebolehpercayaan, analisis faktor dan analisis korelasi. Penerangan seterusnya melibatkan perincian proses-proses yang telah dilaksanakan bagi menghasilkan model kesedaran keselamatan maklumat. Proses yang terlibat termasuklah pengesahan instrumen kajian, pelaksanaan kaji selidik, pengumpulan dan persediaan data, analisis data dan pengesahan model.

4.2 PENGESAHAN INSTRUMEN KAJIAN

Pengesahan instrumen kajian dilaksanakan secara penilaian pakar menggunakan kaedah temuduga. Pengesahan instrumen kajian memastikan setiap item yang digunakan meliputi semua faktor kesedaran keselamatan maklumat, tiada pertindihan antara satu sama lain dan mudah difahami. Hasil akhir penilaian pakar merupakan instrumen kajian yang telah ditambah baik dan sedia untuk digunakan dalam kajian sebenar.

Pakar yang dipilih melibatkan tiga (3) orang pegawai dalam bidang keselamatan maklumat sektor awam yang mempunyai pengalaman dan kemahiran melebihi 15 tahun dalam bidang pengurusan teknologi maklumat dan keselamatan maklumat. Ketiga-tiga pakar yang dipilih berupaya untuk mengesahkan instrumen awal kajian dalam konteks sektor awam.

Proses pengesahan telah dilaksanakan secara temu bual individu pada 16 dan 17 Januari 2018 yang mengambil masa dalam lingkungan dua (2) jam setiap sesi. Setiap pakar dibekalkan dengan instrumen kajian sebagai rujukan sepanjang sesi. Semua pakar diberi masa secukupnya untuk membaca dan menandakan komen bagi setiap dimensi dan item. Pengkaji berada bersama-sama pakar sepanjang sesi dijalankan bagi menjawab sebarang persoalan yang dibangkitkan.

Sesi penilaian dimulakan dengan menerangkan matlamat dan tujuan diadakan sesi tersebut. Pakar turut dimaklumkan tujuan dan matlamat kajian dibuat bagi memberi pemahaman lebih mendalam berkaitan kajian. Penerangan terperinci seterusnya diberikan berkaitan proses-proses penilaian yang perlu dibuat oleh setiap pakar. Pakar diminta menandakan √ sekiranya bersetuju atau X sekiranya tidak bersetuju pada semua dimensi dan item yang disenaraikan.

Soalan turut dikemukakan kepada pakar untuk mendapatkan justifikasi bagi dimensi dan item yang tidak dipersetujui. Pakar juga dibenarkan untuk menambah atau menghapuskan dimensi dan item berdasarkan pengalaman dan pengetahuan masing-masing. Ruangan catatan turut disediakan bagi membolehkan pakar membuat sebarang catatan yang berkaitan.

Seterusnya di akhir sesi penilaian, maklum balas setiap pakar dibincangkan dengan terperinci. Bagi maklum balas yang bercanggah, analisis lanjut dibuat bersama-sama antara pakar dan pengkaji bagi membolehkan konsensus dibuat di mana hanya satu (1) jawapan yang dianggap paling bersesuaian direkodkan.

Pakar juga telah bersetuju dengan penggunaan pengukuran Likert dengan skala lima (5) sebagai skala pengukuran bagi item yang digunakan. Semua pakar yang ditemu bual telah memberikan kerjasama yang baik sepanjang sesi dijalankan.

Berdasarkan penilaian pakar, instrumen kajian telah dikemas kini secara terperinci daripada segi kandungan dan juga format sebelum digunakan dalam kajian sebenar. Instrumen kaji selidik hasil penilaian kesemua pakar adalah seperti di Lampiran B.

4.3 PELAKSANAAN KAJI SELIDIK

Kaedah tinjauan telah digunakan bagi mengumpul data daripada responden secara rawak. Instrumen kaji selidik telah diagihkan secara dalam talian menggunakan perkhidmatan *Google Survey* dan juga luar talian (edaran secara manual). Responden merupakan penjawat awam yang bertugas di Ibu Pejabat Suruhanjaya Pilihan Raya Malaysia (SPR) Putrajaya. Responden telah diberi masa secukupnya untuk melengkapkan instrumen kaji selidik.

Setiap responden dihubungi melalui e-mel yang turut mengandungi surat permohonan mendapatkan kerjasama responden untuk melengkapkan instrumen kaji selidik yang disertakan. Pendekatan adalah secara kuantitatif dan kualitatif kerana kajian melibatkan penyediaan borang soal seidik kepada responden dan temuduga bersama pihak pakar yang telah dilakukan bagi mendapatkan instrumen kajian yang telah disahkan.

4.3.1 Persampelan

Persampelan dilaksanakan secara persampelan kebarangkalian (rawak) ke atas populasi penjawat awam di Ibu Pejabat Suruhanjaya Pilihan Raya Malaysia (SPR) Putrajaya. Populasi terdiri daripada pengguna yangg berjumlah dalam anggaran 200 orang.

Sampel dihadkan kepada responden yang bertugas di Ibu Pejabat Suruhajaya Pilihan Raya Malaysia Putrajaya sahaja kerana mengambil kira faktor kekangan masa dan skop kajian.

4.3.2 Kajian Rintis

Kajian rintis dijalan bagi memastikan kesahihan dan kebolehpercayaan item-item dalam borang soal selidik. Ianya merupakan satu percubaan awal terhadap teknik dan prosedur sebenar. Menurut Abdul Ghafar (2003), satu kajian rintis perlu dijalan sebelum kajian sebenar dilaksana dengan menggunakan sampel yang mempunyai ciri-ciri yang serupa dengan populasi yang hendak diuji. Ini bagi memastikan kajian yang dijalan mempunyai kesahihan dan kebolehpercayaan yang tinggi dan sebaliknya.

Kajian rintis yang dibuat merupakan satu langkah pra-kajian di mana kelemahan-kelemahan yang terdapat dalam borang soal selidik dapat dikenalpasti dan sebarang penambahbaikkan boleh dibuat. Kajian rintis juga bertujuan untuk mengenalpasti masalah berhubung dengan pemahaman responden terhadap soal selidik yang dibuat oleh pengkaji. Item-item soal selidik digubal oleh pengkaji untuk mendapatkan maklumat daripada responden, maka kajian rintis dilaku bagi menentukan kebolehpercayaan soal selidik tersebut.

Tahap kebolehpercayaan item diukur menggunakan nilai *Cronbach's coefficient alpha* (CA) yang dibangunkan oleh (Cronbach 1951). Nilai CA dinyatakan dalam julat 0 hingga 1. Interpretasi nilai CA dikelaskan kepada enam (6) kategori iaitu, melebihi 0.9 (cemerlang), melebihi 0.8 (baik), melebihi 0.7 (boleh diterima), melebihi 0.6 (diragui), melebihi 0.5 (lemah) dan kurang daripada 0.5 (tidak boleh diterima) (George, & Mallery 2003). Nilai CA 0.7 ditetapkan sebagai nilai minimum kebolehpercayaan (DeVellis 2003; Lee et al. 2002; Nunnally 1978).

Merujuk kepada Baker (1994), saiz sampel di antara 10% hingga 20% daripada saiz sampel sebenar adalah jumlah yang munasabah yang dipertimbang dalam kajian

rintis. Oleh yang demikian, kajian rintis bagi kajian dijalan terhadap lima belas (15) penjawat awam. Analisis keputusan kajian rintis dibuat dengan menggunakan perisian SPSS (*Statistical Package for Social Science*) versi 24.

Merujuk kepada Jadual 4.1, didapati kesemua nilai-nilai *Cronbach Alpha* yang diperolehi melebihi 0.8. Ini bermakna item-item yang dibentuk adalah baik (Cronbach 1951).

Jadual 4.1 Skor *Cronbach-Alpha* dari kajian rintis

Bil	Dimensi	Skor
1.	Sikap	0.815
2.	Sokongan Pihak Pengurusan	0.831
3.	Latihan dan Pendidikan	0.823
4.	Polisi/Dasar Keselamatan Maklumat	0.867
5.	Kesedaran Keselamatan Maklumat	0.939

4.4 PENGUMPULAN DAN PERSEDIAAN DATA

Seramai 64 orang responden telah melengkapkan kaji selidik melalui perkhidmatan kaji selidik atas talian *Google*, manakala maklum balas 68 orang responden diterima secara luar talian (edaran secara manual). Data yang diperolehi telah diproses menggunakan perisian SPSS. Proses persediaan data melibatkan pengenalpastian data tidak diisi (data tanpa nilai) dan pengekodan jawapan responden bagi setiap item.

Berdasarkan analisis deskriptif yang dibuat menggunakan perisian SPSS, tiada data tidak diisi (data tanpa nilai) dikesan. Ini disebabkan kesemua item adalah wajib dilengkapkan oleh responden. Seterusnya proses pengekodan jawapan bagi setiap item dibuat kecuali Bahagian A sahaja. Item yang dikodkan merupakan item yang akan digunakan untuk analisis statistik seterusnya. Manakala item Bahagian A tidak dikodkan kerana hanya melibatkan analisis deskriptif sahaja.

Jawapan bagi setiap item yang diperolehi daripada soal selidik adalah dalam bentuk teks iaitu berdasarkan skala pengukuran yang digunakan iaitu sangat tidak setuju (1), tidak setuju (2), tidak pasti (3), setuju (4), sangat setuju (5). Bagi membolehkan ujian statistik dijalankan ke atas data yang dikumpul, proses pengekodan telah dibuat menggunakan perisian SPSS di mana jawapan bagi setiap item dikodkan ke dalam format nombor. Pengekodan dibuat berdasarkan Jadual 4.1.

Jadual 4.1 Kod jawapan item

Skala Pengukuran Dalam Format Teks	**Kod bagi Item**
Sangat tidak setuju	1
Tidak setuju	2
Tidak pasti	3
Setuju	4
Sangat setuju	5

4.5 ANALISIS DESKRIPTIF

Analisis deskriptif dijalankan bertujuan untuk mendapatkan gambaran secara menyeluruh berkaitan data yang diperolehi melalui kaji selidik. Analisis deskriptif dibahagikan kepada dua (2) bahagian iaitu analisis deskriptif bagi maklumat umum responden (Bahagian A) dan dimensi kesedaran keselamatan maklumat (Bahagian B).

Bagi analisis deskriptif bahagian A, peratusan responden berdasarkan jantina, umur, tempoh tahun perkhidmatan dalam kerajaan, tempoh perkhidmatan di agensi sekarang, klasifikasi perkhidmatan, kelayakan akademik tertinggi dan kumpulan perkhidmatan dianalisis bagi melihat keseimbangan agihan responden. Keseimbangan agihan penting untuk memastikan data yang dikumpulkan tidak menjurus kepada kumpulan tertentu sahaja.

Manakala bagi analisis deskriptif bahagian B, maklumat min, mod dan median bagi setiap item dianalisis untuk melihat agihan persepsi responden berdasarkan lima (5) skala Likert yang digunakan. Analisis deskriptif ini dapat memberi gambaran awal tahap persetujuan responden terhadap kesedaran keselamatan maklumat.

Maklumat bagi analisis deskriptif dipersembahkan dalam bentuk rajah dan jadual bagi membantu pemahaman. Penerangan lanjut berkaitan analisis deskriptif ditunjukkan dalam bahagian berikutnya. Manakala, bagi Bahagian C, cadangan yang dikemukakan oleh responden direkodkan dan disediakan di akhir bab ini.

4.5.1 Maklumat Umum

a) Jantina

Bagi taburan responden berdasarkan jantina, bilangan responden perempuan ialah sebanyak 61.4% berbanding bilangan responden lelaki yang hanya 38.6%. Taburan berdasarkan jantina adalah seperti Jadual 4.3.

Jadual 4.3 Bilangan Responden Mengikut Jantina

Jantina	**Bilangan**	**Peratusan**
Lelaki	51	38.6%
Perempuan	81	61.4%
Jumlah	**132**	**100.00%**

b) Umur

Peratusan responden mengikut umur pula menunjukkan responden dalam lingkungan umur 35-44 tahun merupakan majoriti iaitu sebanyak 43.9%, diikuti umur 25-34 tahun sebanyak 29.5%, diikuti umur <= 24 tahun sebanyak 13.6%,

diikuti umur 45-54 tahun sebanyak 9.8% dan yang terakhir ialah 3% bagi umur >= 55 tahun. Jadual 4.4 memaparkan taburan responden mengikut umur.

Jadual 4.4 Bilangan Responden Mengikut Umur

Umur	**Bilangan**	**Peratusan**
<=24 Tahun	18	13.6%
25 hingga 34 Tahun	39	29.5%
35 hingga 44 Tahun	58	43.9%
45 hingga 55 tahun	13	9.8%
>= 55 Tahun	4	3.0%
Jumlah	**132**	**100.00%**

c) Tempoh Tahun Perkhidmatan Dalam Kerajaan

Analisis deskriptif bagi tempoh tahun perkhidmatan dalam kerajaan menunjukkan menunjukkan responden dalam lingkungan tempoh tahun 11-20 tahun merupakan majoriti iaitu sebanyak 37.9%, diikuti tempoh tahun 6-10 tahun sebanyak 25%, diikuti tempoh tahun <= 1 tahun sebanyak 14.4%, diikuti tempoh tahun >=21 tahun sebanyak 12.1% dan yang terakhir ialah 10.6% bagi tempoh tahun 1-5 tahun. Jadual 4.5 memaparkan taburan responden mengikut tempoh tahun perkhidmatan dalam kerajaan.

Jadual 4.5 Bilangan Responden Mengikut Tempoh Perkhidmatan Dalam Kerajaan

Tempoh Perkhidmatan	**Bilangan**	**Peratusan**
< 1 Tahun	19	14.4%
1 hingga 5 Tahun	14	10.6%
6 hingga 10 Tahun	33	25.0%
11 hingga 20 Tahun	50	37.9%
>= 21 Tahun	16	12.1%
Jumlah	**132**	**100%**

d) Tempoh Perkhidmatan di Organisasi Sekarang

Analisis deskriptif bagi tempoh tahun perkhidmatan di organisasi sekarang menunjukkan menunjukkan responden dalam lingkungan tempoh tahun 1-5 tahun merupakan majoriti iaitu sebanyak 31.1%, diikuti tempoh tahun 6-10 tahun sebanyak 29.5%, diikuti tempoh tahun <= 1 tahun sebanyak 25%, diikuti tempoh tahun 11-20 tahun sebanyak 11.4% dan yang terakhir ialah 3% bagi tempoh tahun >=21 tahun. Jadual 4.6 memaparkan taburan responden mengikut tempoh perkhidmatan di organisasi sekarang.

Jadual 4.6 Bilangan Responden Mengikut Tempoh Perkhidmatan di Organisasi Sekarang

Tempoh Perkhidmatan	**Bilangan**	**Peratusan**
< 1 Tahun	33	25.0%
1 hingga 5 Tahun	41	31.1%
6 hingga 10 Tahun	39	29.5%
11 hingga 20 Tahun	15	11.4%
>= 21 Tahun	4	3.0%
Jumlah	**132**	**100%**

e) Klasifikasi perkhidmatan

Analisis deskriptif bagi klasifikasi perkhidmatan menunjukkan menunjukkan responden N-Pentadbiran & Sokongan merupakan kumpulan majoriti iaitu sebanyak 45.5%, diikuti F-Teknologi Maklumat sebanyak 27.3%, diikuti M-Tadbir dan Diplomatik sebanyak 13.6%, diikuti W-Kewangan sebanyak 6.8%, diikuti S-Sosial/Pustakawan sebanyak 3.8% dan yang terakhir ialah 3% bagi lain-lain klasifikasi perkhidmatan. Jadual 4.7 memaparkan taburan responden mengikut klasifikasi perkhidmatan.

Jadual 4.7 Bilangan Responden Mengikut Klasifikasi Perkhidmatan

Klasifikasi Perkhidmatan	Bilangan	Peratusan
M- Tadbir dan Diplomatik	18	13.6%
F-Teknologi Maklumat	36	27.3%
N-Pentadbiran & Sokongan	60	45.5%
S-Sosial/ Perpustakaan	5	3.8%
W-Kewangan	9	6.8%
Lain-lain	4	3.0%
Jumlah	**132**	**100.00%**

f) Kelayakan Akademik

Analisis deskriptif bagi kelayakan akademik menunjukkan menunjukkan responden Sarjana Muda merupakan kumpulan majoriti iaitu sebanyak 37.1%, diikuti Diploma/STPM sebanyak 35.6%, diikuti SPM sebanyak 18.9%, diikuti Sarjana sebanyak 6.8% dan yang terakhir ialah 1.5% bagi kelayakan akademik PMR/PT3. Jadual 4.8 memaparkan taburan responden mengikut kelayakan akademik.

Jadual 4.8 Bilangan Responden Mengikut Kelayakan Akademik

Kelayakan Akademik	Bilangan	Peratusan
Sarjana	9	6.8%
Sarjana Muda	49	37.1%
Diploma/ STPM	47	35.6%
SPM	25	18.9%
PMR	2	1.5%
Jumlah	**132**	**100.00%**

g) Kumpulan perkhidmatan

Analisis deskriptif bagi kumpulan perkhidmatan menunjukkan responden Sokongan Gred 17-26 merupakan kumpulan majoriti iaitu sebanyak 37.1%, diikuti Sokongan Gred 27-40 sebanyak 31.8%, diikuti Pengurusan & Profesional Gred 41-44 sebanyak 22%, diikuti Pengurusan & Profesional Gred

48-54 sebanyak 5.3% dan yang terakhir ialah 3.8% bagi Sokongan Gred 1-16. Jadual 4.9 memaparkan taburan responden mengikut kumpulan perkhidmatan.

Jadual 4.9 Bilangan Responden Mengikut Kumpulan Perkhidmatan

Kumpulan Perkhidmatan	Bilangan	Peratusan
Pengurusan & Profesional Gred 48-54	7	5.3%
Pengurusan & Profesional Gred 41-44	29	29%
Sokongan Gred 27 hingga 40	42	42%
Sokongan Gred 17 hingga 26	49	49%
Sokongan Gred 1 hingga 16	5	5%
Jumlah	**132**	**100.00%**

4.5.2 Dimensi Kesedaran Keselamatan Maklumat

Terdapat lima (5) dimensi yang dikaji iaitu sikap, sokongan pihak pengurusan, latihan dan pendidikan, polisi/dasar keselamatan maklumat dan kesedaran keselamatan maklumat. Analisis maklumat min, median dan mod dilaksanakan bagi mendapatkan taburan skor secara keseluruhan. Bahagian berikutnya menerangkan analisis deskriptif bagi setiap dimensi.

a) Sikap

Dimensi sikap mengukur sejauh mana sikap berhubungkait dengan kesedaran keselamatan maklumat. Terdapat lima (5) item yang mengukur dimensi ini. Berdasarkan Jadual 4.10 menunjukkan nilai min bagi item A1, A2, A3, A4 dan A5 berada dalam lingkungan empat (4), yang bermaksud secara puratanya responden setuju bahawa sikap memainkan peranan dalam kesedaran keselamatan maklumat.

Nilai median dan mod adalah dalam julat empat (4) hingga lima (5) bagi semua item.

Jadual 4.10 Analisis deskriptif dimensi sikap

Item	Min	Median	Mod
A1 Saya tidak berkongsi katalaluan dengan orang lain	4.76	5	5
A2 Saya tidak membuka sisipan (attachment) emel dari penghantar yang tidak dikenali.	4.40	5	5
A3 Saya tidak memuat turun sebarang fail/perisian yang diragui ke dalam komputer	4.57	5	5
A4 Saya senantiasa memastikan perisian antivirus di komputer dalam keadaan terkini	4.32	4	4
A5 Saya sedar isu keselamatan maklumat adalah tanggungjawab semua pekerja di agensi	4.69	5	5

b) Sokongan Pihak Pengurusan

Dimensi sokongan pihak pengurusan mengukur sejauh manakah pihak pengurusan membantu mempertingkatkan tahap kesedaran keselamatan maklumat dalam kalangan pekerja. Terdapat lima (5) item yang mengukur dimensi ini. Berdasarkan Jadual 4.11 menunjukkan nilai min bagi semua item hampir sama iaitu dalam lingkungan empat (4), yang bermaksud secara puratanya responden bersetuju bahawa pihak pengurusan membantu dalam mempertingkatkan kesedaran keselamatan maklumat dalam kalangan pekerja. Nilai median dan mod bagi semua item adalah sama iaitu empat (4).

Jadual 4.11 Analisis deskriptif dimensi sokongan pihak pengurusan

Item	Min	Median	Mod
B1 Pihak pengurusan memastikan pekerja mematuhi arahan keselamatan maklumat	4.36	4	4
B2 Pihak pengurusan memperuntukan bajet bagi menyediakan latihan berkaitan keselamatan maklumat kepada pekerja	4.04	4	4
B3 Pihak pengurusan mengadakan kempen kesedaran keselamatan maklumat dari semasa ke semasa kepada pekerja	4.11	4	4
B4 Pihak pengurusan mengedarkan pekeliling/ polisi/dasar berkaitan keselamatan maklumat kepada pekerja	4.24	4	4
B5 Pihak pengurusan melantik pegawai keselamatan maklumat bagi mengawal selia keselamatan maklumat agensi	4.25	4	4

c) Latihan Dan Pendidikan

Dimensi latihan dan pendidikan mengukur sejauh manakah latihan dan pendidikan membantu menambahkan kefahaman berkaitan isu keselamatan maklumat. Terdapat lima (5) item yang mengukur dimensi ini. Berdasarkan Jadual 4.12 menunjukkan nilai min bagi item C1,C2,C3 dan C5 adalah dalam lingkungan empat (4), kecuali bagi item C4 iaitu dalam lingkungan tiga (3).

Ini bermaksud secara puratanya responden bersetuju bahawa latihan dan pendidikan adalah penting bagi menambah kefahaman. Nilai median dan mod semua item agak sekata iaitu dalam julat empat (4) kecuali item C4 iaitu dua (2).

Jadual 4.12 Analisis deskriptif dimensi latihan dan pendidikan

Item	Min	Median	Mod
C1 Saya perlu menghadiri latihan berkaitan keselamatan maklumat	4.30	4	4
C2 Pihak pengurusan menyediakan latihan berkaitan keselamatan maklumat kepada pekerja	4.02	4	4
C3 Pihak pengurusan menyalurkan maklumat keselamatan melalui kempen dan latihan	4.02	4	4
C4 Pihak pengurusan perlu menyediakan latihan keselamatan maklumat secara dalam talian (*online)* kepada pekerja	3.00	2	2
C5 Kefahaman berkaitan isu keselamatan maklumat bertambah jika saya menghadiri seminar/latihan	4.28	4	4

d) Polisi / Dasar Keselamatan Maklumat

Dimensi polisi/dasar keselamatan maklumat mengukur sejauh manakah polisi/dasar dapat membantu dalam meningkatkan kesedaran keselamatan maklumat dalam kalangan pengguna. Terdapat lima (5) item yang digunakan untuk mengukur dimensi ini. Berdasarkan Jadual 4.13 menunjukkan nilai min bagi item D1, D2, D3 dan D5 agak sekata iaitu dalam lingkungan empat (4), yang bermaksud secara puratanya responden bersetuju maklumat digambarkan secara konsisten.

Walau bagaimanapun, nilai min bagi item D4 lebih rendah iaitu 3.99. Nilai median dan mod bagi semua item agak sekata iaitu empat (4).

Jadual 4.13 Analisis deskriptif dimensi polisi/dasar keselamatan maklumat

Item	Min	Median	Mod
D1 Agensi menyediakan polisi keselamatan maklumat sebagai rujukan pekerja	4.12	4	4
D2 Polisi keselamatan maklumat diedarkan kepada semua pekerja	4.11	4	4
D3 Polisi keselamatan maklumat adalah bertujuan untuk meminimumkan kesan insiden keselamatan maklumat di agensi	4.31	4	4
D4 Polisi keselamatan dikemaskini dari semasa ke semasa bersesuaian dengan isu terkini	3.99	4	4
D5 Polisi keselamatan menjadi bahan rujukan apabila membuat keputusan berkaitan keselamatan maklumat	4.17	4	4

e) Kesedaran Keselamatan Maklumat

Dimensi kesedaran keselamatan maklumat mengukur sejauh manakah tahap kesedaran keselamatan maklumat dalam kalangan pengguna. Terdapat lima (5) item yang digunakan untuk mengukur dimensi ini. Berdasarkan Jadual 4.14 menunjukkan nilai min bagi semua item adalah dalam lingkungan empat (4), yang menggambarkan secara puratanya responden bersetuju berkaitan kepentingan kesedaran keselamatan maklumat.

Nilai median pula adalah empat (4). Manakala nilai mod pula menunjukkan nilai empat (4).

Jadual 4.14 Analisis deskriptif dimensi kesedaran keselamatan maklumat

Item	Min	Median	Mod
E1 Saya tahu apa yang dimaksudkan dengan isu keselamatan maklumat	4.29	4	4
E2 Saya tahu apa itu ancaman keselamatan maklumat	4.34	4	4
E3 Saya mematuhi polisi keselamatan yang disediakan oleh pihak pengurusan	4.28	4	4
E4 Saya memastikan semua fail/perisian yang dimuat turun bebas virus	4.25	4	4
E5 Saya melaporkan kepada pihak pengurusan sekiranya terdapat tanda-tanda ancaman keselamatan maklumat di agensi	4.41	4	4

4.6 PENGUKURAN NORMALITI DATA

Pengukuran normaliti data dibuat bagi menentukan ujian statistik yang boleh dilaksanakan. Normaliti data diukur bagi keseluruhan sampel yang diperolehi menggunakan perisian SPSS. Normaliti data diukur berdasarkan output SPSS yang menyediakan maklumat seperti nilai *skewness*, nilai *kurtosis* dan graf histogram bagi taburan skor. Bahagian berikut menerangkan pengukuran normaliti data yang telah dijalankan.

4.6.1 Nilai *Skewness* dan *Kurtosis*

Nilai *skewness* memberi indikasi sama ada taburan data adalah simetri atau tidak simetri. Manakala nilai *kurtosis* memberi maklumat berkaitan *peakedness* bagi taburan data. Sekiranya taburan skor adalah normal, nilai *skewness* dan *kurtosis* bersamaan 0.

Nilai *skewness* positif bermakna skor adalah terkumpul pada bahagian kiri yang mempunyai nilai yang rendah. Manakala nilai *skewness* negatif bermaksud skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi.

Bagi nilai *kurtosis* pula, nilai positif memberi indikasi bahawa taburan skor adalah terkumpul pada bahagian tengah yang mempunyai ekor yang kurus dan panjang. Manakala nilai *kurtosis* kurang daripada 0 menunjukkan taburan adalah mendatar di mana banyak kes berada pada nilai ekstrem.

Jadual 4.15 menunjukkan nilai *skewness* dan nilai *kurtosis* bagi dimensi sikap. Nilai *skewness* lebih banyak memberi nilai negatif yang memberi indikasi bahawa taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi. Nilai *kurtosis* juga menunjukkan lebih kepada nilai positif yang memberi indikasi bahawa taburan skor adalah terkumpul pada bahagian tengah yang mempunyai ekor yang kurus dan panjang.

Jadual 4.15 Nilai *skewness* dan *kurtosisi* sikap

Sikap	Sikap1	Sikap2	Sikap3	Sikap4	Sikap5
Skewness	-1.473	-1.444	-.817	-.415	-1.203
Ralat Piawai	.211	.211	.211	.211	.211
Kurtosis	.868	2.014	-.376	-.691	.291
Ralat Piawai	.419	.419	.419	.419	.419

Jadual 4.16 menunjukkan nilai *skewness* dan nilai *kurtosis* bagi dimensi sokongan pihak pengurusan. Nilai *skewness* lebih banyak memberi nilai negatif yang memberi indikasi bahawa taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi. Nilai *kurtosis* juga menunjukkan lebih kepada nilai positif yang memberi indikasi bahawa taburan skor adalah terkumpul pada bahagian tengah yang mempunyai ekor yang kurus dan panjang.

Jadual 4.16 Nilai *skewness* dan *kurtosis* sokongan pihak pengurusan

Pengurusan	Urus1	Urus2	Urus3	Urus4	Urus5
Skewness	-.572	-.061	-.875	-.948	-.883
Ralat Piawai	.211	.211	.211	.211	.211
Kurtosis	.561	-1.185	1.954	2.111	.650
Ralat Piawai	.419	.419	.419	.419	.419

Jadual 4.17 menunjukkan nilai *skewness* dan nilai *kurtosis* bagi dimensi latihan dan pendidikan. Nilai *skewness* lebih banyak memberi nilai negatif yang memberi indikasi bahawa taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi. Nilai *kurtosis* juga menunjukkan lebih kepada nilai positif yang memberi indikasi bahawa taburan skor adalah terkumpul pada bahagian tengah yang mempunyai ekor yang kurus dan panjang.

Jadual 4.17 Nilai *skewness* dan *kurtosis* latihan dan pendidikan

Latihan	Latih1	Latih2	Latih3	Latih4	Latih5
Skewness	-.693	-.754	-.709	.760	-.644
Ralat Piawai	.211	.211	.211	.211	.211
Kurtosis	1.333	.910	.800	-1.312	1.589
Ralat Piawai	.419	.419	.419	.419	.419

Jadual 4.18 menunjukkan nilai *skewness* dan nilai *kurtosis* bagi dimensi polisi/dasar keselamatan maklumat. Nilai *skewness* lebih banyak memberi nilai negatif yang memberi indikasi bahawa taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi. Nilai *kurtosis* juga menunjukkan lebih kepada nilai negatif yang memberi indikasi bahawa taburan skor adalah mendatar dan berada pada nilai yang ekstrem.

Jadual 4.18 Nilai *skewness* dan *kurtosis* polisi/dasar keselamatan maklumat

Polisi	Polisi1	Polisi2	Polisi3	Polisi4	Polisi5
Skewness	-.434	-.134	-.166	-.185	-.525
Ralat Piawai	.211	.211	.211	.211	.211
Kurtosis	-.164	-.816	-.594	-.814	.097
Ralat Piawai	.419	.419	.419	.419	.419

Jadual 4.19 menunjukkan nilai *skewness* dan nilai *kurtosis* bagi dimensi kesedaran keselamatan maklumat. Nilai *skewness* lebih banyak memberi nilai negatif yang memberi indikasi bahawa taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi. Nilai *kurtosis* juga menunjukkan lebih kepada nilai positif yang memberi indikasi bahawa taburan skor adalah terkumpul pada bahagian tengah yang mempunyai ekor yang kurus dan panjang.

Jadual 4.19 Nilai *skewness* dan *kurtosis* kesedaran keselamatan maklumat

Kesedaran	Sedar1	Sedar2	Sedar3	Sedar4	Sedar5
Skewness	-.425	-.438	-.368	-.316	-.277
Ralat Piawai	.211	.211	.211	.211	.211
Kurtosis	.600	.787	.767	-.735	-.820
Ralat Piawai	.419	.419	.419	.419	.419

4.6.2 Taburan Skor Keseluruhan Dimensi

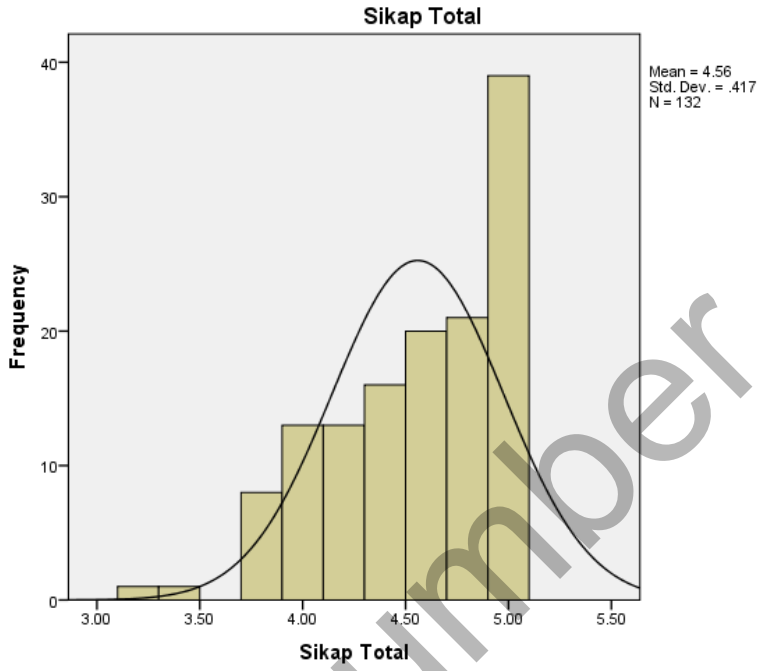
Taburan skor adalah normal sekiranya nilai min, median dan mod hampir sama. Berdasarkan Jadual 4.20 menunjukkan nilai min, median dan mod hampir sama iaitu dalam julat empat (3) hingga lima (5).

Jadual 4.20 Nilai min, median dan mod keseluruhan dimensi

Dimensi	**Min**	**Median**	**Mod**
Sikap	4.5591	4.6000	5.00
Sokonga Pihak Pengurusan	4.1985	4.0000	4.00
Latihan dan Pendidikan	3.9227	3.8000	3.60
Polisi/Dasar Keselamatan Makumat	4.1409	4.0000	4.00
Kesedaran Keselamatan Maklumat	4.3136	4.0000	4.00

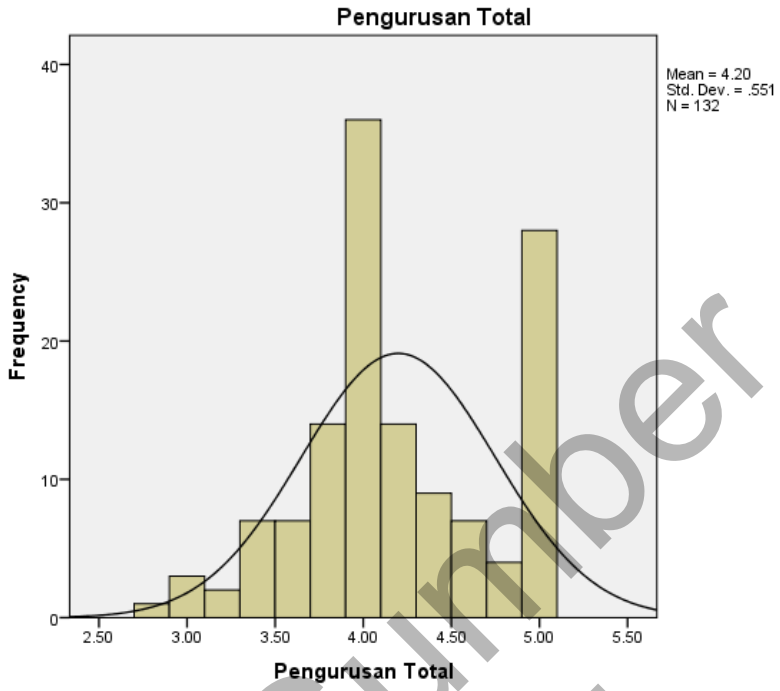
Seterusnya, bentuk sebenar taburan skor ditunjukkan melalui paparan graf histogram.

Rajah 4.1 menunjukkan taburan min skor bagi dimensi sikap. Taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi.



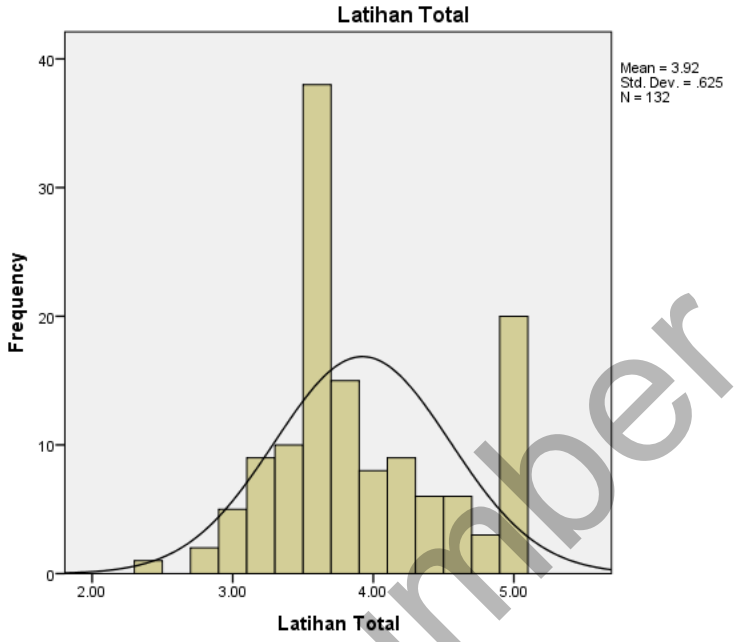
Rajah 4.1 Histogram taburan min skor Sikap

Rajah 4.2 menunjukkan taburan min skor bagi dimensi sokongan pihak pengurusan. Taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi.



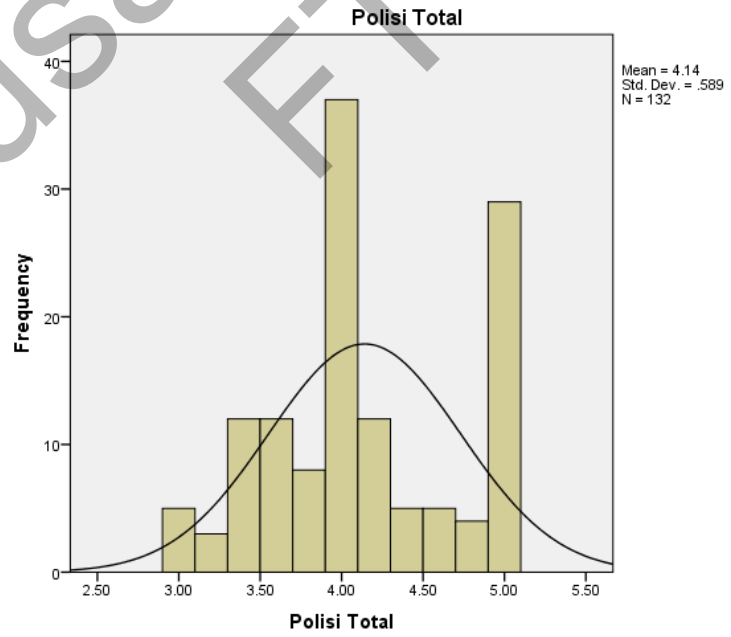
Rajah 4.2 Histogram taburan min skor Sokongan Pihak Pengurusan

Rajah 4.3 menunjukkan taburan min skor bagi dimensi latihan dan pendidikan. Taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi



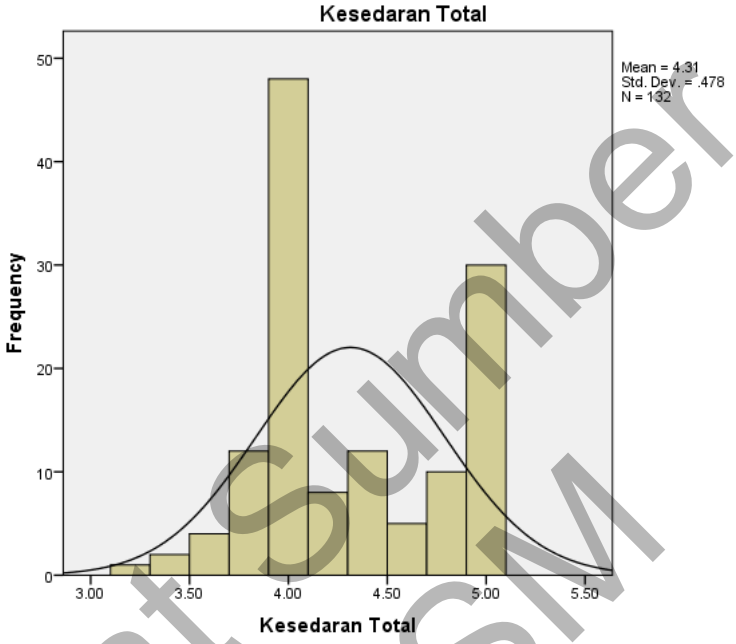
Rajah 4.3 Histogram taburan min skor Latihan Dan Pendidikan

Rajah 4.4 menunjukkan taburan min skor bagi dimensi polisi/dasar keselamatan maklumat. Taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi



Rajah 4.4 Histogram taburan min skor Polisi/Dasar Keselamatan Maklumat

Rajah 4.5 menunjukkan taburan min skor bagi dimensi kesedaran keselamatan maklumat. Taburan skor adalah tidak normal di mana skor adalah terkumpul pada bahagian kanan yang mempunyai nilai yang lebih tinggi.



Rajah 4.5 Histogram taburan min skor Kesedaran Keselamatan Maklumat

4.7 UJIAN KEBOLEHPERCAYAAN

Ujian kebolehpercayaan dilaksanakan untuk menilai konsistensi dalaman item berdasarkan darjah korelasi di antara setiap item dalam mengukur dimensi yang sama. Ujian kebolehpercayaan juga dapat menentukan nilai ralat rawak yang mungkin wujud dalam pengukuran (Nunnally & Bernstein 1994). Ujian kebolehpercayaan dilaksanakan bagi kesemua lima (5) dimensi kesedaran keselamatan maklumat.

Hasil ujian kebolehpercayaan adalah seperti yang ditunjukkan di Jadual 4.21. Berdasarkan jadual tersebut menunjukkan dimensi polisi/dasar keselamatan maklumat dan kesedaran keselamatan maklumat memperolehi nilai CA melebihi 0.9 (cemerlang).

Dimensi sokongan pihak pengurusan dan latihan dan pendidikan memperolehi nilai CA di antara 0.8 hingga 0.89 (baik). Dimensi sikap memperolehi nilai CA 0.713 iaitu dalam kategori boleh diterima.

Jadual 4.21 Ujian kebolehpercayaan CA

Bil	Dimensi	Skor
1	Sikap	0.713
2	Sokongan Pihak Pengurusan	0.817
3	Latihan Dan Pendidikan	0.862
4	Polisi / Dasar Keselamatan Maklumat	0.913
5	Kesedaran Keselamatan Maklumat	0.929

4.8 ANALISIS FAKTOR

Analisis faktor merupakan salah satu teknik statistik yang digunakan untuk mengenal pasti dan memahami struktur hubung kait item bagi setiap dimensi (Gorsuch 1983; Kim & Mueller 1978). Walaupun ujian kebolehpercayaan menunjukkan wujud hubung kait atau konsistensi yang tinggi antara item di bawah dimensi yang sama, namun analisis faktor masih perlu dilaksanakan kerana kemungkinan wujud lebih daripada satu (1) dimensi bagi item yang dikelompokkan di bawah dimensi yang sama (Gliem & Gliem 2003).

Analisis faktor dibuat bagi kesemua lima (5) dimensi yang dikaji. Jadual 4.22 menunjukkan keputusan analisis faktor bagi semua dimensi. Maklumat terperinci ujian analisis faktor adalah seperti di Lampiran E.

Jadual 4.22 Ujian Analisis Faktor

Dimensi	Item 1	Item 2	Item 3	Item 4	Item 5
Sikap	.716	.709	.775	.548	.728
Sokonga Pihak Pengurusan	.740	.771	.846	.815	.749
Latihan dan Pendidikan	.655	.805	.824	.704	.774
Polisi/Dasar Keselamatan Makumat	.857	.878	.800	.862	.848
Kesedaran Keselamatan Maklumat	.834	.833	.836	.767	.733

4.9 ANALISIS KORELASI

Analisis korelasi dilaksanakan untuk menguji dan menerangkan arah serta kekuatan hubungan antara setiap dimensi yang dikaji. Arah hubungan dibahagikan kepada dua (2) jenis, arah positif (+) bermaksud peningkatan pada satu dimensi memberi kesan kepada peningkatan dimensi yang lain dan sebaliknya. Manakala arah negatif (-) bermaksud peningkatan pada satu dimensi mengurangkan dimensi yang lain dan sebaliknya.

Kekuatan hubungan pula diterangkan berdasarkan nilai korelasi Spearman yang terhasil berdasarkan Cohen (1988) seperti di Jadual 4.23.

Jadual 4.23 Kekuatan hubungan berdasarkan nilai korelasi Spearman

Nilai Korelasi	Kekuatan Hubungan
0.1 hingga 0.25	Lemah
0.26 hingga 0.50	Baik
0.51 hingga 0.75	Sangat Baik
0.76 hingga 0.99	Kuat
1.00	Sempurna

Analisis korelasi telah dijalankan untuk menerangkan arah serta kekuatan hubungan antara 5 dimensi kesedaran keselamatan maklumat. Analisis korelasi yang dijalankan mampu menjawab persoalan kajian pertama iaitu adakah wujud hubungan antara setiap dimensi kesedaran keselamatan maklumat.

4.9.1 Analisis Korelasi antara Dimensi

Analisis korelasi antara dimensi kesedaran keselamatan maklumat dibuat bagi menguji dan menerangkan arah serta kekuatan hubungan bagi empat (4) dimensi keselamatan maklumat dengan satu (1) dimensi kesedaran keselamatan maklumat. Hasil korelasi adalah seperti di Jadual 4.24.

a) Sikap

Bagi dimensi A (sikap), kebanyakan korelasi adalah positif baik. Terdapat satu (1) korelasi positif sangat baik dengan dimensi E (kesedaran keselamatan maklumat). Tiada korelasi positif lemah dan kuat. Hasil korelasi menunjukkan bahawa sikap mempunyai hubungan yang sangat baik dan kuat terhadap kesedaran keselamatan maklumat.

b) Sokongan Pihak Pengurusan

Bagi dimensi B (sokongan pihak pengurusan), kebanyakan korelasi adalah positif sangat baik. Terdapat satu (1) korelasi positif baik dan kuat. Tiada korelasi positif lemah. Hasil korelasi menunjukkan bahawa sokongan pihak pengurusan mempunyai hubungan yang sangat baik terhadap kesedaran keselamatan maklumat.

c) Latihan Dan Pendidikan

Bagi dimensi C (latihan dan pendidikan), kebanyakan korelasi adalah positif sangat baik. Walau bagaimanapun, terdapat satu (1) korelasi positif baik iaitu dengan dimensi A. Tiada korelasi positf lemah dan kuat. Hasil korelasi menunjukkan bahawa latihan dan pendidikan mempunyai hubungan yang sangat baik terhadap kesedaran keselamatan maklumat.

d) Polisi/ Dasar Keselamatan Maklumat

Bagi dimensi D (polisi/dasar keselamatan maklumat), kebanyakan korelasi adalah positif sangat baik dan terdapat satu (1) korelasi positif baik dan kuat. Tiada korelasi positif lemah. Hasil korelasi menunjukkan bahawa polisi/dasar keselamatan maklumat mempunyai hubungan yang kuat terhadap kesedaran keselamatan maklumat.

e) Kesedaran Keselamatan Maklumat

Bagi dimensi E (kesedaran keselamatan maklumat), semua korelasi adalah positif sangat baik di mana tiada korelasi positif lemah, positif baik dan kuat. Hasil korelasi menunjukkan dimensi E (kesedaran keselamatan maklumat)

mempunyai korelasi yang sangat baik dengan kesemua dimensi kesedaran keselamatan maklumat.

Jadual 4.24 Korelasi antara dimensi

Kod	Dimensi	Arah dan Kekuatan				
		Positif Lemah	**Positif Baik**	**Positif Sangat Baik**	**Positif Kuat**	**Tiada korelasi**
A	Sikap	Tiada	B (.441) C (.349) D (.498)	E (.568)	Tiada	Tiada
B	Sokongan Pihak Pengurusan	Tiada	A (.441)	C (.610) E (.513)	D (.762)	Tiada
C	Latihan Dan Pendidikan	Tiada	A (.349)	B (.610) D (.601) E (.513)	Tiada	Tiada
D	Polisi/Dasar Keselamatan Maklumat	Tiada	A (.498)	C (.601) E (.529)	B (.762)	Tiada
E	Kesedaran Keselamatan Maklumat	Tiada	Tiada	A (.568) B (.513) C (.516) D (.529)	Tiada	Tiada

Secara keseluruhannya, hasil analisis korelasi antara dimensi menunjukkan wujud hubungan sangat baik dan kuat antara setiap dimensi kesedaran keselamatan maklumat. Hasil analisis korelasi antara dimensi sikap, sokongan pihak pengurusan, latihan dan pendidikan serta polisi/dasar keselamatan maklumat dengan dimensi kesedaran keselamatan maklumat menunjukkan semua dimensi mempunyai hubungan yang sangat baik. Analisis korelasi ini telah menjawab persoalan pertama kajian iaitu adakah wujud hubungan antara dimensi keselamatan maklumat dengan dimensi kesedaran keselamatan maklumat iaitu di tahap yang sangat baik dan kuat.

4.10 CADANGAN

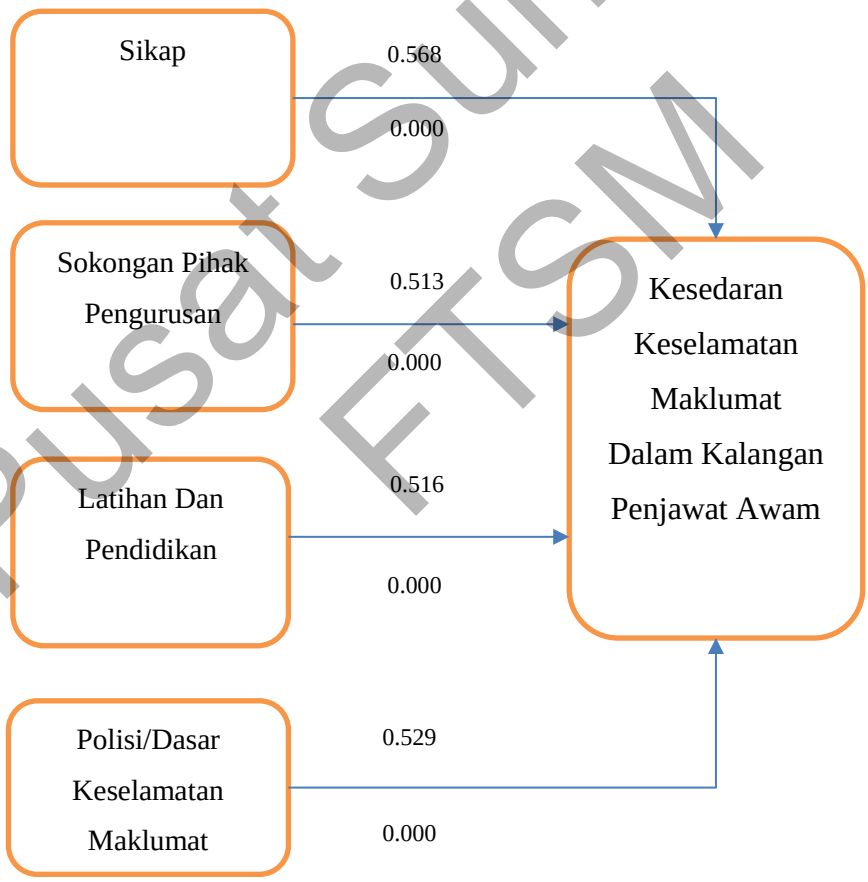
Pada Bahagian C di dalam borang soal selidik, pengguna berpeluang untuk memberi pandangan atau cadangan bagi tujuan penambahbaikan kesedaran keselamatan maklumat. Seramai 11 orang pengguna telah memberi maklumbalas seperti di Jadual 4.25.

Jadual 4.25 Cadangan / Maklumbalas pengguna

Mengikut Dimensi	**Cadangan/Maklumbalas Pengguna**
Sikap	1. Penggunaan wifi di agensi perlu dipantau dan terhad kepada tujuan bekerja. Banyak salah guna wifi bagi kegunaan peribadi. 2. Pengguna tidak boleh melayari laman web yang tidak berkaitan dengan tugas rasmi semasa waktu bekerja.
Sokongan Pihak Pengurusan	3. Personel bahagian keselamatan maklumat mesti lebih berketrampilan untuk memberi kesedaran kepada kakitangan. 4. Pihak pengurusan perlu menjadikan kehadiran kursus sebagai syarat untukpengesahan jawatan.
Latihan dan Pendidikan	5. Perlu selitkan slot peringatan panduan keselamatan pada perhimpunan pagi agensi/jabatan/kementerian. 6. Setiap pegawai baru yang mendaftar di kementerian/jabatan perlu dimaklumkan tentang polisi/garis panduan keselamatan maklumat di organisasi yang berkenaan 7. Latihan dan kursus keselamatan perisaian perlu diadakan sekurang-kurangnya setahun sekali
Polisi/ Dasar Keselamatan Maklumat	8. Pastikan perisian anti virus dikemaskini setap 3 bulan. 9. Semua pekerja mesti dibekalkan dengan polisi keselamatan maklumat semasa lapor diri di tempat kerja. 10. Sebarang kemaskini polisi mesti di maklum dengan kadar segera kepada pekerja melalui laman web atau emel.
Kesedaran Keselamatan Maklumat	11. Kesedaran Keselamatan Maklumat perlu disebarkan melalui media massa dengan lebih kerap dan tidak hanya tertumpu melalui pekeliling jabatan/agensi sahaja.

4.11 PENGESAHAN MODEL OLEH PAKAR

Pada peringkat ini, borang pengesahan pakar seperti dalam Lampiran D telah digunakan untuk mendapatkan pengesahan daripada pihak pakar dalam bidang keselamatan maklumat. Pakar merupakan seorang pegawai teknologi maklumat dari pihak MAMPU. Beliau telah berkhidmat dan berpengalaman lama dalam bidang keselamatan maklumat iaitu melebihi dua puluh (20) tahun. Beliau dipilih kerana beliau bertugas sebagai pegawai yang bertanggungjawab ke atas keselamatan data, rangkaian dan maklumat sektor awam. Cadangan model akhir tersebut adalah seperti yang ditunjukkan dalam Rajah 4.6.



Rajah 4.6 Model Akhir Tahap Kesedaran Keselamatan Maklumat Dalam Kalangan Penjawat Awam

4.12 KESIMPULAN

Hasil analisis data telah membuktikan bahawa wujud hubungan bagi semua dimensi kesedaran keselamatan maklumat dan seterusnya berjaya menghasilkan Model Akhir Tahap Kesedaran Keselamatan Maklumat dalam konteks kajian.

BAB V

RUMUSAN DAN KESIMPULAN

5.1 PENGENALAN

Rumusan dan kesimpulan kajian merangkumi penemuan yang diperolehi berdasarkan kajian kesusasteraan dan ujian empirikal yang telah dilaksanakan. Selain daripada itu, bab ini akan mengulas berkenaan pencapaian objektif kajian, sumbangan kajian dan juga cadangan dan kajian pada masa depan.

5.2 RUMUSAN DAN PENEMUAN KAJIAN

Sejajar dengan perkembangan teknologi dan juga kepentingan maklumat dalam menyokong pelaksanaan tugasan harian, impak kesedaran keselamatan maklumat ke atas prestasi organisasi perlu ditekankan. Sebagai pemangkin kejayaan organisasi, kesedaran keselamatan maklumat dalam kalangan pekerja khususnya penjawat awam perlulah sentiasa ditambahbaik seiring dengan perubahan yang berlaku ke atas organisasi. Perubahan yang berlaku ke atas organisasi ialah sesuatu yang mandatori di mana kegagalan untuk bertindak seiring dengan arus perubahan akan memberi kesan buruk kepada prestasi organisasi.

Kesedaran keselamatan maklumat merupakan salah satu faktor yang penting dalam menentukan kejayaan dalam menjaga kerahsiaan maklumat organsiasi. Kegagalan untuk menilai dan menambah baik kesedaran keselamatan maklumat secara langsung memberi kesan kepada prestasi organisasi.

Sehubungan dengan itu, kajian ini dijalankan bertujuan untuk mencapai dua objektif utama iaitu: