DASAR KESELAMATAN ICT PKPMP

PEJABAT KETUA PENDAFTAR
MAHKAMAH PERSEKUTUAN MALAYSIA

Versi Dokumen: 4.0
Nombor Dokumen: PKPMP-BTM-ISMS-P1-001

A. INFORMASI DOKUMEN

Jenis Dokumen: Manual Keselamatan	**Nombor Dokumen:** PKPMP-BTM-ISMS-P1-001	**Rujukan Fail:** PKPMP-100-15/1/1
	Versi Dokumen: 4.0	**Tarikh Berkuatkuasa:** 11 Mac 2024
Disediakan Oleh: Yusri Hakim bin Yeop (Penolong Pengarah Kanan BTM) Tarikh : 11 Mac 2024	**Disemak Oleh:** Rummie Wisning (Pengarah BTM) Tarikh : 11 Mac 2024	**Diluluskan Oleh:** Azhaniz Teh bin Azman Teh (Timbalan Ketua Pendaftar) Tarikh : 11 Mac 2024
Pengedaran Dokumen BTM		

B. REKOD PINDAAN

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
1.1	10/12/2010	Salinan Pertama		
2.0	06/01/2015	Salinan Kedua Pindaan keseluruhan Bidang Keselamatan dengan merujuk kepada Standard ISO/IEC 27001:2013 *Information Security Management System* (ISMS)	m/s : 74-75	Jawatankuasa Pemandu ICT Jawatankuasa Pemandu ICT Bil 6/2014
2.1	01/06/2017	Salinan Ketiga Pindaan pada Lampiran 1 Surat Akuan Pematuhan DKICT PKPMPM & Lampiran 2 Surat Akuan Pematuhan DKICT PKPMPM (Pembekal) Pindaan pada bidang 050201 Pendaftaran Pengguna dan Pembatalan Pengguna	m/s : 25	Jawatankuasa Pemandu ICT

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
3.0	28/09/2020	Salinan Keempat Pindaan keseluruhan Bidang Keselamatan dengan merujuk kepada Standard ISO/IEC 27001:2013 *Information Security Management System* (ISMS)	Semua	Jawatankuasa Pemandu ICT
3.1	26/11/2020	Mengemas kini polisi di dalam dasar keselamatan DKICT berdasarkan penemuan audit dalaman ISMS : - Tambahan info - Pengeculian Pematuhan DKICT dan Prosedur ICT - Borang Pengecualian Pematuhan Dasar Keselamatan ICT di PKPMP - 080401 Jejak Audit - 080404 *Clock Synchronisation*	7.0 / ms 15 Lampiran 4 ms 39 ms 40	Jawatankuasa Pemandu ICT
3.2	01/04/2022	Mengemas kini perkara-perkara di bawah:		Jawatankuasa Pemandu ICT

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
		- Penambahan media storan – *cloud storage* - 010102 kekerapan semakan DKICT - 040101 Penyataan semula b) dan c) - 050301 kekerapan penukaran kata laluan (j) - 050403 kekerapan penukaran kata laluan (g) - 070105 perekodan keluar masuk ke Pusat Data - 070206 penambahan penyataan bagi peralatan keluar premis - 090203 penambahan item (f) - Menyelaraskan kesemua lampiran	ms 3 ms 9 ms 20 ms 28 ms 29 ms 34 ms 37 ms 49 Lampiran	
3.3	10/08/2022	Mengemaskini perkara berikut:		Jawatankuasa Pemandu ICT

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
		i. Nama Fail ii. Format dokumen iii. Menambah perkataan "dan/atau" pada perkara 050301	A / ms ii Lampiran 1-5 ms 26	
4.0	11/03/2024	i. Menambah perkataan 'Infrasturktur Sokongan' ii. Penambahan kawalan baru iaitu *Threat Intelligent, Secure Coding, Cloud Service, Data Masking, Information Deletion* dan *Data Leakage Prevention* iii. Polisi bagi 'Pematuhan' ditukar menjadi Bidang 17	4.0 / ms 3 ms 21, 22, 51, 62, 63, 64 ms 65	Jawatankuasa Pemandu ICT

KANDUNGAN

1.0 PENGENALAN

Dasar Keselamatan ICT (DKICT) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) Pejabat Ketua Pendaftar Mahkamah Persekutuan Malaysia (PKPMP). Peraturan-peraturan ini perlu difahami dan dipatuhi oleh semua pengguna di PKPMP. Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT PKPMP.

2.0 OBJEKTIF

Objektif utama Dasar Keselamatan ICT di PKPMP adalah seperti berikut:

a. Memastikan isu keselamatan dan perlindungan Sumber ICT dikendalikan dengan baik dan berkesan bagi memastikan kerahsiaan, integriti, ketersediaan, kesahihan maklumat dan komunikasi terpelihara;
b. Melindungi kepentingan pihak-pihak yang bergantung kepada penggunaan Sumber ICT daripada kesan kegagalan atau ancaman keselamatan;
c. Memastikan kesinambungan perkhidmatan dan kelancaran operasi PKPMP sentiasa pada tahap yang paling optimum;
d. Mencegah dan melindungi Sumber ICT daripada sebarang ancaman; dan
e. Meminimumkan kerosakan, kemusnahan dan kos sekiranya berlaku kegagalan dan ancaman.

3.0 PERNYATAAN DASAR KESELAMATAN ICT PKPMP

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan bagi segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a. Melindungi maklumat rahsia rasmi dan maklumat rasmi di PKPMP 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 hanya kepada pengguna yang sah atau penerimaan maklumat dari sumber-sumber yang sah.

DKICT PKPMP merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a. Kerahsiaan – maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran;
b. Integriti – data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;
c. Tidak boleh disangkal – punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
d. Kesahihan – data dan maklumat hendaklah dijamin kesahihannya; dan
e. Kebolehsediaan – data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semulajadi aset ICT, risiko yang mungkin timbul dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

4.0 SKOP

Sistem ICT PKPMP terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT dan data. PKPMP telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

a. Data dan Maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.
b. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan PKPMP.

Bagi menentukan sistem ICT ini terjamin keselamatannya sepanjang masa, DKICT PKPMP ini merangkumi perlindungan ke atas semua bentuk maklumat ICT Kerajaan yang dimasuki, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dan dibuat salinan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a. Data dan maklumat – semua data dan maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT;
b. Peralatan ICT – semua peralatan komputer dan periferal seperti komputer peribadi, stesen kerja, kerangka utama dan alat-alat prasarana seperti *Uninterrupted Power Supply* (UPS);
c. Infrastruktur sokongan – semua mata kuasa, genset dan pendingin hawa;
d. Media Storan – semua media storan dan peralatan yang berkaitan seperti *cloud storage* PKPMP (AWAN), disket, *thumbdrive,* CD ROM, pita, cakera, pemacu cakera, kad memori dan *external hard disk*;
e. Komunikasi dan peralatan rangkaian – semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway*, *bridge*, *router* dan peralatan PABX;
f. Perisian – semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan mengirim maklumat. Ini meliputi semua perisian sistem, perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data, fail program dan fail data;
g. Dokumentasi – semua dokumentasi yang mengandungi maklumat berkaitan dengan penggunaan dan pemasangan peralatan dan perisian. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, *transparencies*, risalah dan slaid-slaid;

h. Manusia – semua pengguna yang dibenarkan termasuk pentadbir dan pengurus serta mereka yang bertanggungjawab terhadap keselamatan ICT; dan
i. Premis komputer dan komunikasi – semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) hingga (g) di atas.

Dasar ini terpakai kepada semua Pengguna ICT di PKPMP yang mencapai, mengurus, menyelenggara, memproses, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT PKPMP.

5.0 PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT PKPMP dan perlu dipatuhi adalah seperti berikut:

a. Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

b. Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

c. Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT PKPMP hendaklah menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka. Akauntabiliti atau tanggungjawab pengguna termasuklah:

a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
b. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
c. Menentukan maklumat sedia untuk digunakan;
d. Menjaga kerahsiaan kata laluan;
e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d. Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

e. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f. Pematuhan

Dasar Keselamatan ICT PKPMP hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

g. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan; dan

h. Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

6.0 PENILAIAN RISIKO KESELAMATAN ICT

PKPMP hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu PKPMP perlu mengambil langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

PKPMP hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat PKPMP termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, pusat pemulihan bencana, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

PKPMP bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. PKPMP perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a. mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b. menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
c. mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
d. memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

7.0 PENGECUALIAN KRITERIA

Permohonan pengecualian dasar keselamatan ICT dan prosedur ICT boleh dibuat dengan melengkapkan borang Pengecualian Pematuhan Dasar Keselamatan ICT dan Prosedur ICT (PKPMP-BTM-ISMS-P1-001-B004) beserta justifikasi dan faedah yang dikaitkan dengan penafian. Permohonan pengecualian ini perlu mendapat kelulusan Jawatankuasa Pemandu ISMS. Pengecualian polisi ISMS tersebut hanya boleh digunakan dalam situasi yang berkaitan untuk tempoh masa maksimum satu (1) tahun. Pengecualian polisi perlu dinilai semula apabila tamat tempoh satu (1) tahun.

BIDANG 01 **DASAR KESELAMATAN**	
0101 Pengurusan Keselamatan Maklumat ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PKPMP dan perundangan yang berkaitan.	
010101 Dasar Keselamatan Maklumat	
Satu set dasar untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dikomunikasikan oleh pihak pengurusan PKPMP kepada pegawai/staf dan pihak-pihak luar yang relevan. Ketua Pendaftar PKPMP adalah bertanggungjawab terhadap pelaksanaan dasar ini dengan dibantu oleh Jawatankuasa Pemandu ICT (JPICT) PKPMP yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Pengarah Bahagian Teknologi Maklumat, Pengarah Mahkamah Negeri, semua Ketua Bahagian dan pegawai-pegawai yang diturunkan kuasa. Dasar Keselamatan Maklumat perlu menangani keperluan: a. Strategik PKPMP; b. Peraturan, undang-undang dan kontrak; dan c. Ancaman persekitaran keselamatan maklumat semasa dan unjuran Polisi keselamatan maklumat hendaklah mengandungi kenyataan yang membabitkan: a. Definisi keselamatan maklumat, objektif dan prinsip kepada semua aktiviti yang berhubung dengan keselamatan maklumat b. Tanggungjawab am dan khusus bagi pengurusan keselamatan maklumat c. Proses ketidakpatuhan pengendalian dan pengecualian keselamatan maklumat.	Ketua Pendaftar (KP) / Pegawai yang diturunkan kuasa
010102 Kajian Semula Dasar Keselamatan Maklumat	
Dasar Keselamatan Maklumat PKPMP perlu dikaji semula tiga (3) tahun sekali atau apabila perubahan ketara untuk memastikan kesesuaian kesinambungan, kecukupan dan keberkesanan dasar. Setiap dasar keselamatan maklumat harus mempunyai pemilik yang telah diluluskan tanggungjawab pengurusan untuk pembangunan, penilaian dan kajian.	

Kajian semula dasar keselamatan PKPMP perlu menilai peluang untuk penambahbaikan dasar sebagai tindak balas kepada perubahan persekitaran organisasi, keadaan perniagaan dan keadaan undang-undang.	

BIDANG 02 **KESELAMATAN ORGANISASI**	
0201 Struktur Organisasi Keselamatan	
Objektif: Menerangkan peranan dan tanggungjawab pengguna yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.	
020101 Ketua Pendaftar	
Peranan dan tanggungjawab Ketua Pendaftar adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT; b. Merangka, mengkaji semula pelaksanaan dan keberkesanan Dasar Keselamatan ICT mengikut keperluan; c. Memberi arahan dan hala tuju yang jelas serta sokongan pengurusan yang mantap; d. Mewujudkan dan mengetuai Jawatankuasa Pemandu Keselamatan ICT PKPMP; e. Meluluskan pelantikan mana-mana pegawai yang diberi peranan dan tanggungjawab terhadap keselamatan maklumat ICT dalam organisasi; f. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT PKPMP; g. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT PKPMP; h. Memastikan semua keperluan keselamatan ICT jabatan (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; i. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT PKPMP; dan j. Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Dasar Keselamatan ICT. Sila rujuk **Lampiran 1**.	Ketua Pendaftar
020102 Ketua Pegawai Digital (CDO)	
Peranan dan tanggungjawab CDO yang dilantik adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT; b. Bertanggungjawab kepada Ketua Pendaftar dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; c. Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya; d. Menentukan keperluan keselamatan ICT; e. Memastikan dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT;	CDO

f. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT PKPMP; g. Memastikan dan melaksanakan program-program kesedaran mengenai keselamatan ICT; h. Menyelia dan memantau perlaksanaan Dasar Keselamatan ICT di peringkat negeri; i. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT PKPMP; dan j. Menandatangani "Surat Akuan Pematuhan" bagi mematuhi Dasar Keselamatan ICT. Sila rujuk **Lampiran 1**.	
020103 Pengurus ICT	
Pengarah Bahagian Teknologi Maklumat merupakan Pengurus ICT PKPMP. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT PKPMP; b. Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan PKPMP; c. Menentukan kawalan akses semua pengguna terhadap aset ICT PKPMP; d. Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO untuk tindakan; e. Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT PKPMP dilaksanakan; f. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai Pentadbir Sistem ICT yang tamat perkhidmatan, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; g. Menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta melaksanakan langkah perlindungan yang bersesuaian; h. Memaklumkan insiden keselamatan ICT kepada ICTSO; i. Mengenalpasti punca ancaman atau insiden keselamatan ICT dan melaksanakan langkah-langkah membaik pulih dengan segera; j. Melaporkan sebarang salahlaku pengguna yang melanggar dasar keselamatan ICT PKPMP kepada ICTSO; dan k. Menyelaraskan program-program kesedaran mengenai keselamatan ICT.	Pengurus ICT

020104 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan; b. Menguatkuasakan Dasar Keselamatan ICT PKPMP; c. Mengurus keseluruhan program-program keselamatan ICT PKPMP; d. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT PKPMP kepada semua pengguna; e. Menjalankan penilaian risiko; f. Menyelaraskan program audit, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. Melaporkan insiden keselamatan ICT kepada Pasukan Tindakbalas Insiden Keselamatan ICT (GCERT-NACSA) dan memaklumkannya kepada Ketua Jabatan, CDO dan Pengurus ICT; dan i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera.	
020105 Pentadbir Sistem ICT	
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT PKPMP; b. Menjaga kerahsiaan kata laluan; c. Menjaga kerahsiaan konfigurasi aset ICT; d. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT PKPMP; e. Memantau aktiviti capaian harian pengguna; f. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; g. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; dan	Pentadbir Sistem ICT: a.Pentadbir Pusat Data; b.Pentadbir Email; c.Pentadbir Rangkaian; d.Pentadbir Sistem dan Aplikasi

h. Menyimpan dan menganalisis rekod jejak audit (audit trail).	
020106 Pengguna PKPMP	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT PKPMP; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Menjaga kerahsiaan maklumat Kerajaan yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; d. Menjaga kerahsiaan kata laluan; e. Memastikan maklumat berkaitan adalah tepat dan lengkap dari semasa ke semasa; f. Mengambil bahagian dalam program-program kesedaran mengenai keselamatan ICT (sama ada secara langsung atau tidak langsung); dan g. Menandatangani "Surat Akuan Pematuhan" bagi mematuhi Dasar Keselamatan ICT. Sila rujuk **Lampiran 1**.	Pengguna
020107 Pengguna Luar	
Terdiri daripada pembekal, pakar runding dan pihak-pihak yang berkepentingan. Peranan dan tanggungjawab pengguna luar adalah seperti berikut: a. Membaca, memahami dan mematuhi DKICT PKPMP; b. Menjaga kerahsiaan kata laluan yang diberikan; c. Menggunakan kemudahan ICT dengan berpandukan garis panduan yang telah ditetapkan; dan d. Menandatangani Surat Akuan Pematuhan DKICT PKPMP (Lampiran 2) dan Borang Akta Rahsia Rasmi (Lampiran 3).	Penguna Luar
020108 Jawatankuasa Pemandu ICT (JPICT) PKPMP	
Bertanggungjawab memperakui: a. Meluluskan perlaksanaan ISMS; b. Meluluskan perolehan; c. Mengambil maklum status ISMS; d. Mengesahkan status kemajuan ISMS; e. Melantik Jawatankuasa Pemandu dan Pasukan Kerja ISMS; dan f. Meluluskan dan mengesahkan DKICT.	JPICT
020109 Pasukan Projek ISMS PKPMP	
Projek Persijilan ISO/IEC 27001:2022 dilaksanakan oleh sebuah pasukan projek yang terdiri dari pegawai-pegawai yang dilantik.	Pasukan Projek ISMS

Struktur Organisasi projek ini telah dipersetujui oleh Ketua Pendaftar. Antara tanggungjawab Pasukan Projek ISMS PKPMP adalah: a. Menghadiri kursus kesedaran standard ISO/IEC 27001:2022; b. Menyediakan dan mengemukakan dasar ISMS, *Statement of Applicability* (SoA), penilaian risiko, *risk treatment plan* dan prosedur-prosedur; c. Melaksana prosedur dan kawalan dalam ISO/IEC 27001:2022; d. Melaksanakan *risk treatment plan;* e. Menyedia kaedah pengukuran keberkesanan kawalan ISMS; f. Mengukur keberkesanan kawalan ISMS; g. Memantau dan menyemak semula ISMS; h. Menjalankan kerja-kerja pentadbiran ISMS seperti dokumentasi, minit mesyuarat dan logistik; i. Merancang dan menyelaras pensijilan ISMS; dan j. Merancang pelan latihan, kompetensi dan kesedaran ISMS.	
020110 Computer Emergency Response Team PKPMP (CERT PKPMP)	
Keanggotaan CERT adalah seperti berikut: Pengerusi : CDO Ahli : ICTSO : (1) Pegawai Teknologi Maklumat (2) Penolong Pegawai Teknologi Maklumat Peranan dan tanggungjawab CERT adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; b. Merekod dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baikpulih minima; d. Menghubungi dan melapor insiden yang berlaku kepada GCERT NACSA samada sebagai input atau untuk tindakan seterusnya; e. Menjalankan penilaian untuk mempastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	CERT PKPMP
020111 Audit Dalaman/Pihak Ketiga PKPMP	
a. Menyediakan jadual audit tahunan, jadual pelaksanaan audit dan senarai semak audit; b. Melaksana Audit Dalam berdasarkan kawalan yang diperlukan dalam ISO/IEC 27001:2022; c. Menyediakan Laporan Audit Dalam ISMS; d. Membentang penemuan Audit Dalam ISMS ke Jawatankuasa Pemandu ISMS;	Pasukan Audit ISMS

e. Menjalankan audit susulan bagi mengesahkan tindakan pembetulan yang dilaksanakan; dan f. Mengemukakan Laporan Audit Susulan kepada Jawatankuasa Pemandu ISMS.	
0202 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan Keselamatan kerja jarak jauh dan penggunaan peranti mudah alih.	
020201 Dasar Peranti Mudah Alih dan Kerja Jarak Jauh	
Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti berikut: a. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; b. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; c. Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT; d. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan e. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	ICTSO, Cawangan Pengurusan Sumber Manusia, Pengurus ICT, Pengguna PKPMP & Pengguna Luar

BIDANG 03 **KESELAMATAN SUMBER MANUSIA**	
0301 Sebelum Perkhidmatan	
Objektif: Memastikan semua pengguna termasuk pengguna PKPMP dan pengguna luar memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
030101 Tapisan (*Screening*)	
Perkara yang mesti dipatuhi termasuk yang berikut: Menjalankan tapisan keselamatan untuk pengguna PKPMP serta pengguna luar yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	ICTSO, Cawangan Pengurusan Sumber Manusia, Pengurus ICT, Pengguna PKPMP & Pengguna Luar
030102 Terma & Syarat Pekerjaan	
Perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan PKPMP serta pengguna luar yang terlibat dalam menjamin keselamatan informasi maklumat. b. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	ICTSO, Cawangan Pengurusan Sumber Manusia, Pengurus ICT, Pengguna PKPMP & Pengguna Luar
0302 Dalam Perkhidmatan	
030201 Tanggungjawab Pengurusan	
Perkara yang perlu dipatuhi termasuk yang berikut: a. Pengurusan ICT PKPMP hendaklah memastikan semua pegawai dan kakitangan PKPMP serta pengguna luar mematuhi dasar keselamatan maklumat PKPMP. b. Memastikan pegawai dan kakitangan PKPMP serta pengguna luar mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh PKPMP;	ICTSO, Cawangan Pengurusan Sumber Manusia, Pengurus ICT, Pengguna PKPMP & Pengguna Luar

030202 Latihan kesedaran dan Pendidikan Keselamatan Maklumat	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Melaksanakan latihan kesedaran dan pendidikan berkaitan dengan pengurusan keselamatan ICT kepada pengguna PKPMP dan pengguna luar (sekiranya perlu) secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. b. PKPMP perlu menyediakan latihan kesedaran dan pendidikan keselamatan ICT sekurang-kurangnya sekali setahun. c. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul bagi menjamin kepentingan keselamatan maklumat. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan dan Sumber Manusia, PKPMP.	ICTSO, Cawangan Pengurusan Sumber Manusia, Pengurus ICT, Pengguna PKPMP & Pengguna Luar
030203 Proses Tatatertib	
Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan PKPMP serta pengguna luar sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan	ICTSO, Cawangan Pengurusan Sumber Manusia, Pengurus ICT, Pengguna PKPMP & Pengguna Luar
0303 Penamatan atau Perubahan Perkhidmatan	
030301 Penamatan atau Perubahan Tanggungjawab Pekerjaan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Tanggungjawab keselamatan maklumat dan tugasannya harus ditentukan dan dimaklumkan kepada pekerja atau kontraktor selepas penamatan atau perubahan perkerjaan. b. Menguruskan urusan keluar, bersara, berhenti, bertukar jabatan, ditamatkan perkhidmatan dan tamat/ ditamatkan kontrak serta pertukaran peranan adalah tanggungjawab pengguna PKPMP dan entiti berkaitan; c. Tanggungjawab untuk melaksanakan penamatan atau perubahan pekerjaan hendaklah ditakrifkan dengan jelas termasuk; i. Perjanjian Kerahsiaan (Non Disclosure Agreement (NDA)) ii. Perubahan dalam terma & syarat penamatan / tanggungjawab iii. Tentukan tempoh akhir pekerjaan	ICTSO, Cawangan Pengurusan Sumber Manusia, Pengurus ICT, Pengguna PKPMP & Pengguna Luar

iv. Tanggungjawab masih sah selepas penamatan d. Memastikan semua aset ICT dikembalikan kepada PKPMP mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan e. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh PKPMP dan/atau terma perkhidmatan.	

BIDANG 04 **PENGURUSAN ASET**	
0401 Akauntabiliti/Tanggungjawab Aset	
Objektif: Untuk mengenal pasti aset bagi memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT PKPMP	
040101 Inventori Aset	
Ketua Jabatan bertanggungjawab memastikan semua aset ICT PKPMP diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a. Aset yang berkaitan dengan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenal pasti dan maklumat aset direkodkan dalam borang harta modal atau inventori dan sentiasa dikemaskinikan; b. Semua aset ICT PKPMP hendaklah direkodkan c. Pelabelan adalah merujuk kepada pekeliling pengurusan aset yang berkuatkuasa; d. Memastikan pengendalian, pelupusan dan pemusnahan aset dikendalikan mengikut prosedur yang diteapkan; dan e. Semakan inventori ke atas aset ICT dan kemudahan pemprosesan maklumat perlu dilakukan sekurang-kurangnya sekali setahun.	Pengguna PKPMP & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos
040102 Hakmilik Aset	
PKPMP perlu memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja.	Pengguna PKPMP & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos
040103 Penerimaan Penggunaan Aset	
PKPMP perlu memastikan peraturan bagi pengunaan aset dan kemudahan pemprosesan maklumat dikenal pasti, didokumenkan dan dilaksanakan. Setiap pengguna bertanggungjawab terhadap semua aset ICT di bawah tanggungjawabnya.	Pengguna PKPMP & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos
040104 Pemulangan Aset	
Semua pengguna PKPMP dan pengguna luar hendaklah memulangkan semua aset kepada PKPMP selepas penamatan pekerjaan, kontrak atau perjanjian.	Pengguna PKPMP & Pengguna Luar,

	Pegawai Aset dan Pengarah Negeri Pusat Kos
0402 Klasifikasi Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian selaras dengan kepentingan organisasi.	
040201 Pengelasan Maklumat	
Maklumat terperingkat hendaklah dikelaskan dan dilabelkan mengikut tahap sensitiviti maklumat. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan yang telah ditetapkan di dalam Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Ketua Pendaftar, CDO dan Pegawai ICT
040202 Pelabelan Maklumat	
Prosedur pelabelan maklumat hendaklah merujuk kepada Akta Rahsia Rasmi dan Arahan Keselamatan.	Ketua Pendaftar, CDO dan Pegawai ICT
040203 Pengendalian Aset	
Prosedur bagi mengendalikan aset hendaklah dibangunkan dan dilaksanakan mengikut skim klasifikasi maklumat yang diguna pakai oleh PKPMP. Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Ketua Pendaftar, CDO dan Pegawai ICT

0403 Pengendalian Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
040301 Pengurusan Media Mudah Alih (*Removal* Media)	
Prosedur pengurusan media mudah alih hendaklah dilaksanakan mengikut skim pengelasan yang diguna pakai oleh PKPMP. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; f. Semua media storan yang mengandungi data terperingkat hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan; g. Pelupusan Aset ICT hendaklah dilaksanakan mengikut Pekeliling Pengurusan Aset Alih Kerajaan yang berkuat kuasa; dan h. Pelupusan maklumat hendaklah mengikut Tatacara Pelupusan Arkib Negara (Akta Arkib Negara 2003 [Akta 629])	CDO, Pegawai ICT dan Pengguna
040302 Pelupusan Media	
Pelupusan media perlu mendapat kelulusan dari pihak pengurusan ICT dan mengikut prosedur PKPMP yang mana berkenaan. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul serta selamat dan dengan kebenaran PKPMP.	CDO, Pegawai ICT dan Pengguna
040303 Pemindahan Media Fizikal	
PKPMP hendaklah memastikan media yang mengandungi maklumat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa proses pemindahan.	CDO, Pegawai ICT dan Pengguna
0404 Pemadaman Data	
Objektif: Mencegah pendedahan maklumat sensitif yang tidak sewajarnya dan mematuhi undang-undang, peraturan dan keperluan kontrak dalam pemadaman data dan maklumat.	

040401 Pemadaman Data	
Terdapat banyak rekod dan dokumen yang perlu disediakan & diselenggara dalam bentuk kertas. Oleh itu, dokumen yang disimpan di atas kertas adalah penting untuk dirincihkan atau dimusnahkan mengikut dasar, supaya semua maklumat dilupuskan dengan betul, mengikut garis panduan PKPMP. Pelupusan dan pemusnahan dilakukan selepas kelulusan pengurus pelupusan. Pegawai hendaklah mengambil berat dan memastikan bukti yang digunakan oleh organisasi tidak dimusnahkan. Pemadaman Data digital berdasarkan Tatacara Pengurusan Aset Tak Ketara dan sanitasi data (CGSO).	Pegawai ICT dan Pengguna
0405 *Data Masking*	
Objektif: Mengehadkan pendedahan data sensitif termasuk maklumat data peribadi (PII), dan mematuhi keperluan undang-undang, peraturan dan kontrak.	
040501 *Data Masking*	
Data Masking ialah teknik yang digunakan untuk mencipta versi data yang kelihatan secara struktur seperti yang asal tetapi menyembunyikan maklumat sensitif. Versi dengan maklumat bertopeng kemudiannya boleh digunakan untuk pelbagai tujuan, seperti latihan pengguna atau ujian perisian. Objektif utama menyembunyikan data adalah untuk mencipta pengganti berfungsi yang tidak mendedahkan data sebenar. Data yang sepatutnya ditutup ialah: • Personal Identifiable Information (PII) Data yang boleh digunakan untuk mengenal pasti individu tertentu. Ini termasuk maklumat seperti nombor kad pengenalan, nombor pasport, kata laluan.	Pembekal

BIDANG 05 **KAWALAN CAPAIAN**	
0501 Keperluan Kawalan Capaian	
Objektif: Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.	
050101 Dasar Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan perkhidamtan dan keselamatan maklumat. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti berikut: a. Keperluan keselamatan aplikasi PKPMP b. Kebenaran untuk menyebarkan maklumat c. Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian d. Undang-undang Malaysia/Persekutuan yang berkaitan dan obligasi kontrak mengenai had akses kepada data atau perkhidmatan e. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; f. Pengasingan peranan kawalan capaian g. Kebenaran rasmi permintaan akses h. Keperluan semakan hak akses berkala i. Pembatalan hak akses j. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat k. Akses *priveleged*	ICTSO, Pengurus ICT dan Pentadbir ICT
050102 Capaian Kepada Rangkaian Dan Perkhidmatan Rangkaian	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari PKPMP. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian PKPMP, rangkaian agensi lain dan rangkaian awam;	ICTSO, Pengurus ICT dan Pentadbir Rangkaian

b. Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
0502 Pengurusan Capaian Pengguna	
Objektif: Memastikan kawalan capaian oleh pengguna yang dibenarkan sahaja.	
050201 Pendaftaran Pengguna dan Pembatalan Pengguna	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian. Proses pendaftaran dan pembatalan pengguna hendak disemak dan dikemaskini sekurang – kurang satu kali (1) setahun. Perkara –perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh PKPMP sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna luar yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada PKPMP terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan dan arahan PKPMP. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Bagi memastikan pengendalian Internet dan e-mel Mahkamah beroperasi dengan sempurna dan berkesan, PKPMP adalah bertanggungjawab: i. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan PKPMP. Pembatalan akaun (pengguna yang tamat perkhidmatan, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat. PKPMP boleh membekukan akaun pengguna, jika perlu, semasa pengguna bercuti panjang, berkursus atau pun menghadapi tindakan tatatertib; ii. Menggunakan perisian pemecahan kata laluan yang dibenarkan untuk mengenal pasti kata laluan pengguna yang lemah dan kemudiannya mencadang dan	Pengguna PKPMP & Pengguna Luar, Pentadbir ICT, Pengurus ICT dan ICTSO

memperakukan ciri-ciri kata laluan yang lebih baik kepada pengguna; dan iii. Menghalang kemasukan maklumat dari laman Internet yang berunsur ganas, lucah, permainan elektronik atas talian, judi dan lain-lain aktiviti yang dilarang.	
050202 Semakan Akses Pengguna (*Provisioning*)	
Satu proses semakan akses penguna perlu dilaksanakan untuk mengkaji semula kebenaran dan pembatalan capaian penguna ke atas semua aplikasi dan perkhidmatan.	Pentadbir ICT, Pengurus ICT dan ICTSO
050203 Pengurusan *Privileged Access Rights*	
Peruntukan dan penggunaan *Privileged Access Rights* perlu dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir ICT, Pengurus ICT dan ICTSO
050204 Pengurusan Kata Laluan Pengguna	
Peruntukan kata-laluan perlu melalui beberapa proses pengurusan formal. a. Pengguna perlu disediakan dengan kata laluan sementara, yang pengguna perlu menukar kata laluan pada penggunaan pertama b. Prosedur perlu diwujudkan untuk mengesahkan identiti pengguna sebelum menyediakan kata laluan yang baru, penggantian atau sementara c. kata laluan sementara perlu diedar kepada pengguna dengan selamat dimana katalaluan tidak beleh diedarkan oleh pihak ketiga dan dalam *clear text* d. kata laluan sementara yang dicipta hendaklah unik dan susah dianggar e. pengguna perlu mengesahkan penerimaan kata laluan f. kata laluan vendor *default* perlu diubah selepas pemasangan sistem atau perisian.	Pengguna PKPMP & Pengguna Luar, Pentadbir ICT, Pengurus ICT dan ICTSO
050205 Kajian Semula Hak Capaian Pengguna	
Pemilik aset ICT PKPMP hendaklah mengkaji semula hak pengguna secara berkala atau sekurang-kurangnya satu (1) kali setahun atau sekiranya terdapat perubahan atau keperluan.	Pentadbir ICT, Pengurus ICT dan ICTSO

050206 Pembatalan atau Pelarasan Hak Akses	
Hak capaian kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data dan maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian, atau diselaraskan apabila berlaku perubahan dalam PKPMP. Pembatalan akaun (pengguna yang tamat perkhidmatan, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat. PKPMP boleh membekukan akaun pengguna, jika perlu, semasa pengguna bercuti panjang, berkursus atau pun menghadapi tindakan tatatertib.	Pentadbir ICT, Pengurus ICT dan ICTSO
0503 Tanggungjawab pengguna	
Objektif: Untuk memastikan pengguna bertanggungjawab untuk melindungi maklumat yang digunakan untuk pengesahihan identiti mereka	
050301 Penggunaan Kata Laluan	
Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahihan identiti. Pengguna perlu: a. Pastikan kata laluan adalah SULIT. b. Kata laluan hendaklah diingat dan TIDAK BOLEH didedahkan dengan apa cara sekalipun; c. Tukar kata laluan apabila terdapat tanda-tanda kebocoran atau kompromi kata laluan. d. Pilih kata laluan yang berkualiti dengan panjang minimum yang mencukupi. e. Tidak menggunakan kata laluan yang sama untuk sistem yang lain. f. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan digit, abjad dan/atau simbol KECUALI bagi perkakasan atau perisian yang mempunyai pengurusan katalaluan yang terhad; g. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; h. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; i. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; j. Kata laluan hendaklah ditukar sekurang-kurangnya sepuluh (10) bulan sekali atau selepas tempoh masa yang bersesuaian; dan	Pengguna PKPMP & Pengguna Luar, dan ICTSO

k. Mengelakkan penggunaan kata laluan yang sama bagi urusan rasmi dan tidak rasmi.	
0504 Kawalan Capaian Sistem dan Aplikasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi	
050401 Had Kawalan Capaian Maklumat	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pentadbir ICT, ICTSO, Pengurus ICT
050402 Prosedur Log-on	
Capaian kepada sistem dan aplikasi hendaklah dikawal oleh prosedur *log-on* mengikut keperluan. PKPMP hendaklah mengenal pasti teknik pengesahan *log-on* yang sesuai iaitu: a. Tidak memaparkan pengenalan sistem atau aplikasi selagi proses *log-on* tidak berjaya. b. Paparkan suatu notis amaran bahawa komputer hanya boleh diakses oleh pengguna yang sahTidak memberikan bantuan mesej semasa prosedur *log-on*. c. Pengesahan *log-on*. d. Perlindungan terhadap *Brute Force log-on*. e. Log “aktiviti *log on*” yang berjaya dan tidak berjaya f. Mengadakan amaran keselamatan jika ada potensi percubaan atau pencerobohan *log-on* berjaya dikesan g. Memaparkan maklumat berikut setelah selesai *log-on* yang berjaya i. Tarikh dan masa *log-on* sebelumnya ii. butir-butir percubaan *log-on* yang tidak berjaya h. Tidak memaparkan kata laluan i. Tidak menghantar kata laluan dalam “*clear-text*” melalui rangkaian j. Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu. k. Menghadkan sesi sambungan sekatan untuk aplikasi yang berisiko tinggi.	Pentadbir ICT, ICTSO, Pengurus ICT
050403 Sistem Pengurusan Kata Laluan	
Sistem pengurusan kata laluan mestilah interaktif dan menjamin kata laluan yang berkualiti a. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan digit, abjad dan simbol KECUALI bagi perkakasan atau perisian yang mempunyai pengurusan katalaluan yang terhad;	Pengguna, Pentadbir ICT, ICTSO, Pengurus ICT

b. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; c. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; d. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula KECUALI bagi perkakasan atau perisian yang mempunyai pengurusan katalaluan yang terhad; e. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; f. Tentukan had masa pengesahan mengikut kesesuaian sistem dan selepas had itu, sesi ditamatkan; g. Kata laluan digalakkan untuk ditukar sepuluh (10) bulan sekali atau selepas tempoh masa yang bersesuaian; dan h. Mengelakkan penggunaan kata laluan yang sama bagi urusan rasmi dan tidak rasmi.	
050404 Pengunaan Utiliti Sistem	
Penggunaan program utiliti yang mungkin mampu mengatasi kawalan sistem dan aplikasi hendaklah dihadkan dan dikawal ketat.	Pentadbir ICT
050405 Kawalan Akses Kepada *Source Code Program*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh BTM, PKPMP. (A.9.4.5 *Access control to program source code*) a. Kakitangan sokongan PKPMP perlu dihadkan akses kepada kod sumber (*source code)* b. Log audit perlu dikekalkan kepada semua akses kepada kod sumber c. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada prosedur kawalan perubahan yang ketat d. Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik PKPMP.	Pentadbir Sistem, Pengurus ICT

BIDANG 06 **KRIPTOGRAFI**	
0601 Kawalan kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
060101 Kawalan Pengunaan Kriptografi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membangun dan melaksanakan peraturan enkripsi untuk melindungi maklumat sensitif menggunakan kaedah kriptografi yang sesuai pada setiap masa; b. Mengenal pasti tahap perlindungan pengunaan kriptografi dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan.	Pengguna PKPMP dan Pentadbir ICT
060102 Pengurusan Kunci Kriptografi *(Key Management)*	
Memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi diguna pakai di PKPMP bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut; dan Setiap urusan transaksi maklumat sensitif secara elektronik hendaklah menggunakan tandatangan digital supaya mendapat perlindungan dan pengiktirafan undang-undang.	Pengguna PKPMP dan Pentadbir ICT

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0701 Keselamatan Kawasan	
Objektif: Mencegah akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat and kemudahan pemprosesan maklumat PKPMP	
070101 Kawalan Kawasan	
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Perkara yang perlu dipatuhi adalah seperti berikut: a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c. Memasang alat penggera atau kamera; d. Menghadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan; h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan dan pelawat yang diberi kebenaran sahaja boleh melalui pintu masuk tersebut; i. Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan mengikut Arahan Keselamatan Kerajaan; j. Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; m. Log bagi kad akses ke pintu-pintu kawalan mestilah disemak sekurang-kurangnya setahun sekali atau sekiranya terdapat keperluan atau perubahan; dan n. Pelawat perlu diiringi oleh kakitangan PKPMP yang berkaitan.	Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK), Bahagian Pengurusan, CDO dan ICTSO

070102 Kawalan Masuk Fizikal	
Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis PKPMP. Perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pegawai dan kakitangan PKPMP hendaklah mempamerkan Pas Keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada PKPMP apabila bertukar, tamat perkhidmatan atau bersara; b. Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; dan c. Kehilangan Pas Keselamatan mestilah dilaporkan dengan segera kepada Bahagian Keselamatan.	Pengguna PKPMP, Pengguna Luar, Bahagian Pengurusan
070103 Kawalan Pejabat, Bilik dan Tempat Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada akses oleh orang luar. b. Penunjuk ke lokasi bilik operasi dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk	ICTSO, Pejabat KPKK dan Bahagian Pengurusan
070104 Perlindungan Terhadap Ancaman Luaran dan Dalaman	
PKPMP perlu merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau dan bencana. (	ICTSO, Pejabat KPKK dan Bahagian Pengurusan
070105 Kawalan Tempat Larangan (*Working In Secure Area*)	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai yang diberi kebenaran sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di PKPMP adalah Pejabat operasi ICT PKPMP, Bilik Server, dan Pusat Data (*Data Centre*). Perkara yang perlu dipatuhi adalah seperti berikut: a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; Pihak lain adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali dengan kebenaran khas PKPMP dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; b. kerja tanpa pengawasan oleh kontraktor di kawasan larangan harus dielakkan ; c. Bilik dalam kawasan larangan perlu dikunci pada setiap masa;	ICTSO, Pejabat KPKK dan Bahagian Pengurusan

d. Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk melainkan dengan kebenaran; dan e. Pengguna PKPMP dan pengguna luar yang perlu berurusan di pusat data dan bilik server hendaklah memaklumkan kepada Pentadbir Pusat Data terlebih dahulu dan merekodkan keluar masuk Pusat Data bagi pengguna PKPMP dan pengguna luar yang tidak kerap berurusan dengan pusat data dan bilik server. f. Bagi Pengguna PKPMP dan Pengguna luar yang kerap berurusan dengan pusat data dan bilik server mereka perlu di daftarkan dala sistem dan rekod pengecaman muka dan cap jari bagi tujuan akses. g.	
070106 Kawasan Penghantaran dan Pemunggahan	
PKPMP hendaklah memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	ICTSO, Pejabat KPKK dan Bahagian Pengurusan
0702 Keselamatan Peralatan ICT	
Objektif: Melindungi peralatan ICT PKPMP dari kehilangan, kerosakan, kecurian dan disalahgunakan.	
070201 Peralatan ICT	
Peralatan ICT hendaklah dijaga dan dikawal selia dengan baik. (Perkara yang perlu dipatuhi adalah seperti berikut: a. Memeriksa dan memastikan semua peralatan ICT di bawah kawalan pengguna berfungsi dengan sempurna; b. Bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan ICT yang telah ditetapkan; d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;	Pengguna PKPMP, Pengguna Luar dan ICTSO

h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; j. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; k. Peralatan ICT yang hilang hendaklah dilaporkan segera kepada pihak Polis, Pengarah Mahkamah Negeri (di mana berkenaan), Ketua Jabatan dan ICTSO; l. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; m. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada *Helpdesk* PKPMP untuk dibaik pulih; n. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; o. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; p. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; q. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; dan r. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.	
070202 Peralatan Sokongan ICT	
a. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; b. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); c. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan d. Semua alat sokongan perlu disemak dan dikemaskinikan dari masa kesemasa (sekurang-kurangnya setahun sekali).	Pengguna PKPMP, Pengguna Luar dan ICTSO

070203 Keselamatan Kabel	
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pentadbir Pusat Data
070204 Penyelenggaraan Peralatan	
Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	Semua Pengguna, Pegawai Aset dan Pengurus ICT
070205 Peralatan Dibawa Keluar Permis	
a. Peralatan ICT yang hendak dibawa keluar dari premis PKPMP untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Pendaftar atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan	Semua Pengguna, Pegawai Aset dan Ketua Jabatan

070206 Keselamatan Peralatan di Luar Premis	
Peralatan yang dibawa keluar dari premis PKPMP adalah terdedah kepada pelbagai risiko. Peralatan yang di bawa keluar dari premis PKPMP merangkumi: a. penggunaan perkakasan secara sementara bagi keperluan mesyuarat, latihan dan sebagainya; b. Penempatan perkakasan secara kekal di sesebuah agensi lain. Perkara yang perlu dipatuhi adalah seperti berikut: c. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan d. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua Pengguna dan Pegawai Aset
070207 Pelupusan Peralatan dan Kitar Semula	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh PKPMP dan ditempatkan di PKPMP. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan PKPMP. Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; f. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori Sistem Pengurusan Aset; g. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan h. Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara seperti berikut:	Semua Pengguna, Pegawai Aset dan Ketua Jabatan

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer yang berkaitan ke mana-mana Bahagian di PKPMP; iii. Memindah keluar dari PKPMP mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab PKPMP; dan v. Pengguna bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
070208 Penjagaan Peralatan Yang Tidak Diguna (*Unattended User Equipment*)	
Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: a. Tamatkan sesi aktif apabila selesai tugas. b. *Log-off* kerangka utama, pelayan dan PC pejabat apabila sesi bertugas selesai. c. PC atau terminal selamat daripada pengguna yang tidak dibenarkan.	Semua Pengguna
070209 Clear Desk dan Clear Screen	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b. Menyimpan bahan-bahan sensitif seperti '*electronic storage media'* dan dokumen terperingkat di dalam laci atau kabinet fail yang berkunci; c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Semua Pengguna

d. E-mel masuk dan keluar hendaklah dikawal; dan e. Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	

BIDANG 08 **PENGURUSAN OPERASI**	
0801 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas kemudahan pemprosesan maklumat	
080101 Pengendalian Prosedur	
Bagi memastikan kemudahan pemprosesan maklumat beroperasi seperti yang telah ditetapkan dan selamat, perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pengurus ICT, Pentadbir ICT dan ICTSO
080102 Kawalan Perubahan	
Tanggungjawab dan tugas perlulah diasingkan untuk mengelakkan perubahan yang tidak dibenarkan atau penyalahgunaan aset PKPMP. Oleh itu, perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua Pengguna, Pengurus ICT dan Pentadbir ICT
080103 Perancangan Kapasiti	
a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan	Pentadbir Sistem, Pentadbir Emel,

bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. ; dan b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Pusat Data dan Pengurus ICT
080104 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi	
a. Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*). b. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pentadbir Sistem dan Pengurus ICT
0802 Perisian Berbahaya (*Protection from Malware*)	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	
080201 Perlindungan dari Perisian Berbahaya	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna perlu merujuk kepada garis panduan yang disediakan. b. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; c. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; d. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; e. Mengemas kini anti virus dengan *pattern* antivirus yang terkini. Pengemaskinian perlu dilakukan sekurang-kurangnya sekali sehari atau apabila terdapat *pattern* terkini; f. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; g. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; h. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi perisian berbahaya;	Semua Pengguna, Pentadbir ICT dan ICTSO

i. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan j. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
0803 *Backup*	
Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.	
080301 Sandaran Maklumat (*Information Backup*)	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara yang perlu dipatuhi adalah seperti berikut: a. Penyediaan *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat; e. Membuat salinan pendua ke atas semua data dan maklumat mengikut kesesuaian operasi; dan f. *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat.	Pengguna PKPMP dan Pentadbir ICT
0804 Log dan Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080401 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti penguna PKPMP yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. a. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: i. Rekod setiap aktiviti transaksi pengguna;	Pengguna PKPMP, Pentadbir Sistem, Pentadbir Emel, Pentadbir Rangkaian dan ICTSO

ii. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; iii. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan iv. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. b. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat. c. Pentadbir hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
080402 Perlindungan Log	
Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan.	Pentadbir Pusat Data, Pentadbir Sistem, Pentadbir Rangkaian, Pentadbir Emel dan ICTSO
080403 Log pentadbir dan Operator	
a. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; b. Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu.; c. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; d. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan e. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada Pegawai Keselamatan Teknologi Maklumat (ICTSO) dan CDO.	Pentadbir Pusat Data, Pentadbir Sistem, Pentadbir Rangkaian, Pentadbir Emel dan ICTSO

080404 *Clock Synchronisation*	
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam PKPMP atau domain keselamatan perlu diselaraskan dengan Masa Standard Malaysia sebagai waktu rujukan utama.	Pentadbir Pusat Data
0805 Kawalan Perisian Operasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
080501 Pemasangan Perisian Pada Sistem Operasi	
a. Pengemaskinian perisian operasi, aplikasi dan *program libraries* hanya boleh dilakukan oleh pentadbir terlatih setelah mendapat kelulusan pengurusan. b. Semakan ke atas senarai perisian asset ICT yang dibenarkan perlu dilakukan sekurang-kurang setahun sekali. c. Sistem operasi hanya boleh memegang "*executable code*" dan tidak kod pembangunan atau penyusun. d. Instalasi perisian hendaklah mendapat kebenaran daripada Pentadbir Sistem ICT dan ICTSO. e. Memastikan penggunaan perisian berlesen yang sah dan perisian tidak berlesen (freeware) yang dibenarkan . f. Penggunaan aplikasi dan sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya. g. Instalasi perisian hendaklah mendapat kebenaran daripada Pentadbir Sistem ICT dan ICTSO. h. Memastikan penggunaan perisian mempunyai lesen sah. i. Setiap konfigurasi ke atas sistem perlu dikawal dan didokumentasikan melalui satu sistem kawalan konfigurasi. Konfigurasi hanya boleh dilaksanakan selepas mendapat persetujuan dari pihak berkaitan. j. Satu "*rollback*" strategi harus diadakan sebelum perubahan dilaksanakan.	Pentadbir Sistem & Pengurus ICT
0806 Kawalan Keterdedahan Teknikal (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
080601 Kawalan dari Ancaman KeterdedahanTeknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;	Pentadbir Sistem

b. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c. Mengambil langkah kawalan untuk mengatasi risiko berkaitan.	
080602 Kawalan Pemasangan Perisian	
a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan pengguna di PKPMP; b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya.	Penguna PKPMP, Pentabir Sistem dan ICTSO
0807 Pertimbangan Audit Sistem Maklumat	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080701 Pematuhan Keperluan Audit/Kawalan Audit Sistem Maklumat	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO & Audit Dalaman

BIDANG 09 **KESELAMATAN KOMUNIKASI**	
0901 Pengurusan Keselamatan Rangkaian	
Objektif: Memastikan perlindungan pemprosesan maklumat dalam rangkaian.	
090101 Kawalan Infrastruktur Rangkaian	
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti berikut: a. Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; d. Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian; f. Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan BTM, PKPMP; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada Pegawai Keselamatan Teknologi Maklumat (ICTSO); h. Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat PKPMP; i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan BTM, PKPMP adalah tidak dibenarkan; k. Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di PKPMP sahaja dan penggunaan modem adalah dilarang sama sekali; l. Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya; m. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan.	Pengguna, Pentadbir Rangkaian dan ICTSO

n. Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian di antara rangkaian PKPMP, rangkaian agensi lain dan rangkaian awam; o. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; p. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; q. Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; r. Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan PKPMP; dan s. Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan PKPMP.	
090102 Keselamatan Perkhidmatan Rangkaian	
Pengurusan bagi semua perkhidmatan rangkaian (*inhouse atau outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenalpasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian. Perkara yang mesti dipatuhi adalah seperti berikut: a. Memastikan keselamatan maklumat organisasi diambil kira dalam setiap perjanjian perkhidmatan rangkaian dengan pihak ketiga; b. Menandatangani perjanjian bertulis untuk melindungi maklumat apabila berlaku pemindahan maklumat organisasi antara PKPMP dengan pihak luar; c. Terma perkongsian maklumat dan perisian di antara PKPMP dengan pihak ketiga hendaklah dimasukkan di dalam perjanjian; d. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi Service Level Agreement (SLA) yang telah dipersetujui; dan e. Mempunyai mekanisme pengurusan insiden sekiranya berlaku insiden keselamatan maklumat.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
090103 Pengasingan rangkaian	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian PKPMP.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
0902 Pemindahan Maklumat	
Objektif: Memastikan keselamatan perpindahan/pertukaran maklumat dan perisian antara PKPMP dan pihak luar terjamin.	

090201 Dasar dan Prosedur Pemindahan Maklumat	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Dasar, prosedur dan kawalan pemindahan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan maklumat melalui sebarang jenis kemudahan komunikasi; b. Terma pemindahan maklumat dan perisian di antara PKPMP dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan maklumat; dan d. Memastikan maklumat yang terdapat dalam e-mel hendaklah dilindungi sebaik-baiknya.	Semua Pengguna, Pentadbir Rangkaian, Pentadbir Emel dan ICTSO
090202 Perjanjian Mengenai Pemindahan Maklumat	
PKPMP perlu mengambil kira keselamatan maklumat organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara PKPMP dengan pihak luar. Perkara yang perlu dipertimbangkan adalah: a. Tanggungjawab pengurusan bagi mengawal penghantaran dan penerimaan maklumat organisasi. b. Prosedur bagi pengesanan maklumat organisasi semasa pemindahan maklumat. c. Tanggungjawab dan liabiliti sekiranya berlaku insiden keselamatan maklumat seperti kehilangan data.	CDO dan Pengurus ICT
090203 Pengurusan Mel Elektronik (E-mel)	
Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003 dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara yang perlu dipatuhi dalam pengendalian e-mel adalah seperti berikut: a. Menggunakan akaun atau e-mel PKPMP bagi urusan rasmi. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh PKPMP; c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa	Semua Pengguna

penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f. Pengguna dinasihatkan menggunakan kaedah inovatif dalam penghantaran fail bersaiz besar(melebihi 10Mb) seperti menggunakan kaedah muat turun fail dengan memaklumkan lokasi Universal Resource Location (URL) dengan memastikan ciri-ciri keselamatan di laksanakan; g. Pengguna dilarang dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; h. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; i. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; j. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; k. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; l. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; m. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan n. Pengguna hendaklah bertanggungjawab ke atas penyelenggaraan *mailbox* masing-masing.	
090204 Kerahsiaan dan *Non-Disclosure* Agreement	
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan dari masa ke semasa.	CDO, BTM dan ICTSO

BIDANG 10 **PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM**	
1001 Keperluan Keselamatan Sistem Maklumat	
Objektif: Memastikan keselamatan maklumat adalah merupakan sebahagian daripada proses pembangunan sistem. Ini merangkumi keperluan keselamatan maklumat apabila menggunakan rangkaian luar.	
100101 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat	
Keperluan keselamatan maklumat bagi pembangunan sistem baru dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: a. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Dasar Keselamatan ICT PKPMP. b. Penyediaan rekabentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan c. Ujian keselamatan hendaklah dilakukan di setiap peringkat pembangunan sistem bagi memastikan kesahihan dan integriti data.	Pemilik Sistem dan Pentadbir Sistem
100102 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum	
Maklumat aplikasi yang melalui rangkaian umum (*public networks*) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*). b. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi. c. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan perkhidmatan ICT. d. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak. e. Liabiliti yang berkaitan dengan mana-mana kes transaksi *fraud*. f. Keperluan insuran	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem
100103 Melindungi Perkhidmatan Transaksi Aplikasi	
Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej. Perkara yang perlu dipertimbangkan adalah seperti berikut:	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem

a. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi b. Memastikan semua aspek transaksi dipatuhi: i. maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan ii. mengekalkan kerahsiaan maklumat iii. mengekalkan privasi pihak yang terlibat iv. Komunikasi antara semua pihak yang terlibat dirahsiakan v. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi c. Pihak yang mengeluar dan mengekalkan pensijilan digital atau tandatangan adalah dilantik oleh Kerajaan.	
1002 Keselamatan Dalam Pembangunan Sistem	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.	
100201 Dasar Keselamatan Dalam Pembangunan Sistem	
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan untuk perkembangan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Keselamatan persekitaran pembangunan b. Panduan keselamatan dalam kitar hayat pembangunan (*development lifecycle*) perisian c. Keselamatan dalam fasa reka bentuk d. Pemeriksaan keselamatan dalam perkembangan projek e. Keselamatan repositori f. Keselamatan dalam kawalan versi g. Keperluan pengetahuan keselamatan dalam pembangunan perisian (*secure coding)* h. Kebolehan pengaturcara untuk mengenalpasti kelemahan dan mencadangkan penambahbaikan dalam pembangunan sistem	Pentadbir Sistem dan ICTSO
100202 Prosedur Kawalan Perubahan Sistem	
Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, didokumentasi dan disahkan sebelum diguna pakai; b. Setiap perubahan kepada sistem pengoperasian perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan agensi;	*Change Control Board* dan Pentadbir Sistem

c. Setiap permohonan perubahan/ penambahbaikan sistem hendaklah menggunakan Borang Permohonan Perubahan (*Change Request*) untuk memantau perubahan/penambahbaikan yang dilaksanakan oleh pengaturcara; dan d. Kawalan perlu dibuat ke atas sebarang perubahan atau pindaan ke atas sistem bagi memastikan ianya terhad mengikut keperluan sahaja.	
100203 Kajian Teknikal Selepas Permohonan Perubahan Platform	
Perubahan platform operasi hendaklah dikaji dan diuji bagi memastikan tiada sebarang masalah yang timbul terhadap operasi atau keselamatan aplikasi. Perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan aplikasi dan prosedur integriti disemak untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform. b. Perubahan platform dimaklumkan dari masa ke semasa bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan. c. Memastikan perubahan yang sesuai dibuat kepada pelan kesinambungan organisasi.	Pentadbir Sistem dan Pengurus ICT
100204 Sekatan Perubahan Pakej Perisian (*Software Packages*)	
Perubahan kepada pakej perisian adalah tidak digalakkan tetapi terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem, Pengurus ICT dan ICTSO
100205 Prinsip Kejuruteraan Keselamatan Sistem (S*ecure System Engineering Principles*)	
Prinsip-prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumentasi, diselenggara dan digunapakai dalam pelaksanaan sistem. Keselamatan perlu diambilkira dalam semua peringkat pembangunan sistem. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari masa ke semasa bagi memastikan keberkesanan kepada keselamatan maklumat.	Pentadbir Sistem dan Pengurus ICT
100206 Keselamatan Persekitaran Pembangunan Sistem	
Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem (*development lifecycle*).	Pentadbir Sistem dan Pengurus ICT
100207 Pembangunan Sistem oleh Pembekal	

Pembangunan sistem oleh pembekal perlu sentiasa dikawal selia dan dipantau. Kod sumber (*source code)* bagi semua aplikasi dan perisian hendaklah menjadi hak milik Kerajaan. *Intellectual property rights* (IPR) aplikasi dan perisian yang dibangun oleh pihak ketiga kepada PKPMP adalah hak milik Kerajaan.	Pentadbir Sistem dan Pengurus ICT
100208 Pengujian Keselamatan Sistem	
a. Pengujian keselamatan sistem hendaklah dijalankan semasa pembangunan. b. Semua sistem baru dan penambahbaikan sistem hendaklah menjalani ujian *Security Posture Assessment* (SPA) termasuk penyediaan jadual terperinci aktiviti, ujian input dan output (*input and output validation*). c. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; d. Mengenalpasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi; e. Membuat semakan pengesahan di dalam aplikasi untuk mengenalpasti sebarang pencemaran maklumat sama ada kerana kesilapan atau disengajakan; dan f. Menjalankan proses semak ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan dan kesesuaian.	Pentadbir Sistem dan ICTSO
100209 Pengujian Penerimaan Sistem	
Penerimaan pengujian semua sistem baru dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai.	Pentadbir Sistem dan ICTSO
1003 Data Ujian	
100301 Perlindungan Data Ujian	
a. Data dan atur cara yang hendak diuji perlu dipilih, dilindungi dan dikawal. b. Pengujian hendaklah dibuat ke atas atur cara yang terkini. c. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem dan Pentadbir Sistem
1004 Kawalan Kod Selamat	
Objektif: Memastikan perisian ditulis dengan selamat dengan mengurangkan potensi kerentanan (vulnerability) keselamatan maklumat di dalam perisian.	
100401 Kawalan Kod Selamat	
Persekitaran pembangunan yang selamat hendaklah dibina di atas infrastruktur IT yang boleh dipercayai dan selamat menggunakan	Pentadbir Sistem ICT PKPMP

perkakasan, perisian dan perkhidmatan serta pembekal yang selamat, berdasarkan kepada KRISA Pengekodan selamat hendaklah termasuk: a) Penurunan kod dan pengeliruan; b) Mengelakkan jalan pintas; c) Pengimbasan automatik dan semakan kod; d) Mengelakkan komponen yang mempunyai kelemahan yang diketahui; dan e) Log dan Pengauditan.	

BIDANG 11 **HUBUNGAN DENGAN PEMBEKAL**	
1101 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	
Objektif: Memastikan perlindungan aset PKPMP yang boleh diakses oleh pembekal	
110101 Dasar Keselamatan Maklumat Untuk Pembekal	
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset PKPMP. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori b. Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal c. Mengawal dan memantau akses pembekal d. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian e. Jenis-jenis obligasi kepada pembekal f. Pelan kontingensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat g. Latihan Kesedaran Keselamatan untuk PKPMP dan pembekal	BTM dan Pembekal
110102 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal	
Semua keperluan keselamatan maklumat hendaklah relevan dan dipersetujui dengan setiap pembekal bagi mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur, maklumat organisasi IT. Perkara-perkara yang perlu diambil kira seperti berikut: a. Penerangan maklumat keselamatan b. Skim klasifikasi maklumat c. Keperluan undang-undang dan peraturan d. Obligasi setiap pihak bagi kawalan akses, pemantauan, pelaporan dan pengauditan e. Penerimaan peraturan penggunaan maklumat oleh pembekal f. Latihan teknikal dan kesedaran keselamatan maklumat g. Tapisan keselamatan pembekal h. Hak untuk mengaudit pembekal i. Kewajipan pembekal mematuhi keperluan keselamatan maklumat	BTM dan Pembekal

110103 Kawalan Rantaian Bekalan Maklumat dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan maklumat dan komunikasi. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan. b. Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada subkontraktor bagi perkhidmatan. c. Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada pembekal-pembekal lain bagi pembekalan produk. d. Melaksanakan satu proses/kaedah pemantauan yang boleh mengesahkan pembekalan produk dan perkhidmatan mematuhi keperluan keselamatan maklumat PKPMP. e. PKPMP hendaklah mengenal pasti komponen produk dan perkhidmatan kritikal dan komponen tambahan. f. Memastikan jaminan dari pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik. g. Menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (*supply chain*) antara organisasi dan pembekal	BTM dan Pembekal
1102 Pengurusan Penyampaian Perkhidmatan Pembekal	
110201 Pemantauan dan Kajian Perkhidmatan Pembekal	
PKPMP hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan b. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan. c. Memaklumkan mengenai insiden keselamatan kepada pembekal dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	BTM dan Pembekal
110202 Pengurusan Perubahan Perkhidmatan Pembekal	
Perkara yang perlu diambilkira adalah seperti berikut: a. Perubahan dalam perjanjian dengan pembekal	BTM dan Pembekal

b. Perubahan yang dilakukan oleh PKPMP bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur c. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan sub-kontraktor.	

BIDANG 12 **PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN**	
1201 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat	
Objektif: Memastikan insiden keselamatan maklumat dikendalikan dengan cepat, teratur dan berkesan bagi meminimumkan kesan insiden dan mengenal pasti komunikasi serta kelemahan apabila berlaku insiden.	
120101 Tanggungjawab dan Prosedur	
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.	ICTSO, Pengurus ICT dan CERT PKPMP
120102 Mekanisme Pelaporan Insiden	
Insiden keselamatan ICT atau ancaman yang mungkin berlaku ke atas aset ICT yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada ICTSO. Sekiranya perlu, ICTSO hendaklah melaporkan kepada GCERT Agensi Keselamatan Negara (NACSA) dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa b. Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa; c. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; d. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; e. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; f. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan g. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di PKPMP adalah seperti Prosedur Pengendalian Insiden Keselamatan Maklumat. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan	Pengguna, ICTSO dan CERT PKPMP

b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam. c. Surat NACSA – Surat Ketua Pengarah Keselamatan Negara – Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Goverment Computer Emergency Response Team (GCERT) oleh Agensi Keselamatan Siber Negara (NACSA) yang bertarikh 28 Januari 2019.	
120103 Melaporkan Kelemahan Keselamatan ICT	
Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat PKPMP dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.	Semua Pengguna
120104 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat	
Aktiviti keselamatan maklumat hendaklah dinilai dan diputuskan sama ada untuk diklasifikasikan sebagai insiden keselamatan maklumat.	ICTSO dan BTM
120105 Pengurusan Maklumat Insiden Keselamatan ICT	
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah ditetapkan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b. Menjalankan kajian forensik sekiranya perlu; c. Menghubungi pihak yang berkenaan dengan secepat mungkin; d. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; e. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; f. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; g. Menyediakan tindakan pemulihan segera; dan h. Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	ICTSO, BTM dan CERT PKPMP
120106 Pengalaman Dari Insiden Keselamatan Maklumat	
Pengetahuan dan pengalaman yang diperolehi daripada menganalisis dan menyelesaikan kes-kes insiden keselamatan maklumat perlu digunakan untuk mengurangkan kemungkinan dan kesan kejadian pada masa depan.	ICTSO, BTM dan CERT PKPMP

120107 Pengumpulan Bahan Bukti	
Perkara yang perlu diambil kira adalah seperti berikut: a. Prosedur untuk mengenal pasti, mengumpul, mendapatkan dan menyimpan bahan bukti hendaklah dibangunkan bagi memastikan bahan bukti dilindungi dan tersedia; dan b. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti.	ICTSO, BTM dan CERT PKPMP

BIDANG 13 **Aspek keselamatan maklumat dalam Pengurusan Kesinambungan Perkhidmatan**	
1301 Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Objektif:Keselamatan maklumat hendaklah diberi penekanan dalam sistem pengurusan kesinambungan organisasi	
130101 Rancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
PKPMP hendaklah membangunkan Pelan Pemulihan Bencana ICT dan mengenal pasti aspek keselamatan maklumat. Ini bertujuan memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan organisasi dan mengenal pasti keselamatan maklumat pada lokasi kesinambungan perkhidmatan. Pelan ini mestilah diluluskan oleh CDO.	CDO dan Pasukan Pemulihan Bencana
130102 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
PKPMP hendaklah mewujud, mendokumentasi, melaksana dan mengekalkan proses, prosedur serta kawalan untuk memastikan tahap keselamatan maklumat bagi kesinambungan perkhidmatan dalam situasi yang terancam. Perkara berikut perlu diberi perhatian: a. Mengenalpasti aspek keselamatan dalam membangunkan pelan kesinambungan keselamatan. b. Mengenalpasti semua aset, tanggungjawab, struktur organisasi dan menetapkan prosedur kecemasan atau pemulihan amalan terbaik; c. Mengenalpasti peristiwa atau ancaman yang boleh mengakibatkan gangguan terhadap proses organisasi; d. Mengenalpasti kemungkinan dan impak gangguan tersebut serta akibatnya terhadap keselamatan ICT; e. Menjalankan analisis impak organisasi; f. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; g. Mendokumentasikan proses dan prosedur yang telah ditetapkan; h. Mengadakan program latihan secara berkala kepada warga PKPMP mengenai prosedur kecemasan; i. Membuat *backup* mengikut prosedur yang ditetapkan; dan j. Menguji, menyelenggara dan mengemaskini Pelan Pemulihan Bencana ICT sekurang-kurangnya setahun sekali.	CDO dan Pasukan Pemulihan Bencana

Pelan Pemulihan Bencana ICT perlu dibangunkan dan hendaklah mengandungi perkara berikut: a. Senarai keperluan keselamatan maklumat dalam membangunkan kesinambungan perkhidmatan b. Senarai aktiviti teras dan aset yang dianggap kritikal mengikut susunan keutamaan; c. Senarai personel PKPMP dan pembekal berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai personel gantian juga hendaklah dikenalpasti bagi menggantikan personel yang tidak dapat hadir untuk menangani insiden; d. Senarai lengkap maklumat yang perlu disalin pendua (*backup*) dan lokasi sebenar penyimpanannya; e. Menetapkan arahan pemulihan maklumat dan kemudahan yang berkaitan; f. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah terancam; g. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan penyambungan semula perkhidmatan mengikut keutamaan; dan h. Menguji tahap keselamatan kesinambungan perkhidmatan Salinan pelan kesinambungan perkhidmatan perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi organisasi untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. PKPMP hendaklah memastikan salinan pelan sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	
130103 Mengkaji, Mengesah dan Menilai Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
PKPMP hendaklah mengkaji, mengesah dan menilai tahap keselamatan maklumat yang diwujudkan dan disimpan di lokasi kesinambungan perkhidmatan.	CDO, Pasukan Pemulihan Bencana dan ICTSO

1302 *Redundancy*	
130201 Ketersediaan Kemudahan Pemprosesan Maklumat	
Kemudahan pemprosesan maklumat PKPMP perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan *redundancy* perlu diuji (*failover test*) keberkesanannya dari masa ke semasa.	ICTSO dan BTM

BIDANG 14 **RISIKAN ANCAMAN (*THREAT INTELLIGENCE*)**	
1401 Risikan Ancaman (*Threat Intelligence*)	
Objektif: Untuk memberi kesedaran tentang persekitaran ancaman organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.	
140101 Risikan Ancaman (*Threat Intelligence*)	
Maklumat mengenai ancaman sedia ada atau baharu hendaklah dikumpulkan daripada sumber luaran dan dalaman, dan dianalisis untuk: a) Memudahkan tindakan sewajarnya diambil untuk mencegah ancaman daripada menyebabkan kemudaratan kepada organisasi; b) Mengurangkan kesan ancaman tersebut; dan c) Dikomunikasi dan dikongsi kepada individu yang berkaitan dalam format yang boleh difahami. Sumber dalaman dan luaran tersebut mestilah relevan, tepat pada masanya dan boleh dipercayai.	ICTSO

BIDANG 15
PENGGUNAAN PERKHIDMATAN *CLOUD*

1501 Keselamatan Maklumat Bagi Penggunaan Perkhidmatan *Cloud*

Objektif: Menentukan dan mengurus keselamatan maklumat dalam penggunaan perkhidmatan *cloud*.

150101 Keselamatan Maklumat Bagi Penggunaan Perkhidmatan *Cloud*	
Peranan dan tanggungjawab dalam persekitaran *cloud* • Tanggungjawab dan peranan keselamatan maklumat yang dikongsi dalam penggunaan *cloud* di PKPMP harus diperuntukkan kepada pihak yang dikenal pasti, didokumenkan, dikomunikasikan dan dilaksanakan oleh kedua-dua pengguna dan pembekal perkhidmatan *cloud*. Mengalih keluar aset pelanggan perkhidmatan *cloud* • Aset pengguna perkhidmatan *cloud* yang berada di premis pembekal perkhidmatan *cloud* harus dialih keluar, dan dikembalikan, jika perlu, tepat pada masanya selepas penamatan terma dan syarat perkhidmatan di PKPMP. Keselamatan operasi pentadbir • Prosedur untuk operasi pentadbiran persekitaran pengkomputeran *cloud* harus ditakrifkan, didokumenkan dan dipantau. Pemantauan untuk Perkhidmatan *cloud* • Pengguna perkhidmatan *cloud* harus mempunyai keupayaan untuk memantau aspek tertentu operasi perkhidmatan *cloud* yang digunakan oleh pengguna perkhidmatan *cloud*. Pengasingan dalam persekitaran maya • Persekitaran maya pengguna perkhidmatan cloud yang berjalan pada pembekal perkhidmatan *cloud* harus dilindungi daripada pelanggan perkhidmatan *cloud* yang lain dan pihak yang tidak dibenarkan.	Pengguna dan Pembekal

BIDANG 16 **PENCEGAHAN KEBOCORAN DATA (DLP)**	
1601 Kawalan Pencegahan Kebocoran Data (DLP)	
Objektif: Untuk mengesan dan mencegah pendedahan dan pengekstrakan maklumat yang tidak dibenarkan oleh individu atau sistem.	
160101 Kawalan Pencegahan Kebocoran Data (DLP)	
a) Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran. b) Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.	Pentadbir sistem ICT

BIDANG 17 **PEMATUHAN**	
1701 Pematuhan Terhadap Keperluan Perundangan dan Perjanjian Kontrak	
Objektif: Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	
170101 Mengenalpasti Undang-Undang dan Perjanjian Kontrak	
Semua keperluan undang-undang berkanun, peraturan dan kontrak yang berkaitan dengan PKPMP perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat. Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga di PKPMP adalah seperti di **Lampiran 5**.	Semua Pengguna
170102 Hak Harta Intelek (*Intellectual Property Rights*-IPR)	
PKPMP akan mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. PKPMP mesti mematuhi: a. Keperluan hakcipta yang berkaitan dengan bahan proprietari, perisian, dan rekabentuk yang diperolehi daripada PKPMP. b. Keperluan perlesenan menghadkan penggunaan produk, perisian, rekabentuk dan bahan-bahan lain yang diperolehi oleh PKPMP. c. PKPMP perlu memastikan pematuhan berterusan dengan sekatan hakcipta produk dan keperluan perlesenan. d. Pengguna tidak dibenarkan daripada menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan.	Semua Pengguna
170103 Perlindungan Rekod	
Rekod-rekod yang penting (fizikal atau media) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, pelepasan yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak, dan keperluan perniagaan. Perkara yang perlu ditimbangkan ialah: a. Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat b. Jadual penyimpanan rekod perlu dikenal pasti c. Inventori rekod	Semua Pengguna
170104 Privasi dan perlindungan maklumat peribadi	
PKPMP perlu mengenal pasti privasi dan melindungan maklumat peribadi penguna dijamin seperti yang ditakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan.	Semua Pengguna

170105 Kawalan Kriptografi	
Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang, dan peraturan-peraturan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi-fungsi kriptografi b. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah direka untuk mempunyai fungsi kriptografi c. Sekatan ke atas penggunaan enkripsi d. Kaedah akses oleh pihak berkuasa Malaysia bagi maklumat enkripsi perkakasan dan perisian.	Semua Pengguna
1702 Kajian Keselamatan Maklumat	
170201 Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat	
Perlaksanan keselamatan maklumat PKPMP hendaklah dikaji secara bebas atau oleh pihak ketiga pada jangka masa yang dirancang atau apabila perubahan ketara berlaku dalam perlaksanaannya.	CDO dan JKP ISMS
170202 Pematuhan Dasar dan Standard/Piawaian	
PKPMP hendaklah membuat kajian semula pematuhan dan prosedur pemprosesan maklumat di dalam kawasan tanggungjawab mereka dengan dasar keselamatan ICT PKPMP dan piawaian yang berkenaan. Kajian teknikal perlu dilakukan dua (2) tahun sekali. Sekiranya kajian semula mengenal pasti ketidakpatuhan, PKPMP perlu; a. Mengenal pasti punca-punca ketidakpatuhan b. Menilai keperluan tindakan untuk mencapai pematuhan c. Melaksanakan tindakan pembetulan yang sewajarnya d. Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa kekurangan dan kelemahan	CDO dan JKP ISMS
170203 Pematuhan Kajian Teknikal	
Sistem maklumat hendaklah dikaji supaya selaras dengan pematuhan dasar dan standard keselamatan maklumat organisasi (eg Kajian *Security Posture Assessment* – SPA). Kajian teknikal perlu dilakukan dua (2) tahun sekali atau mengikut kesesuaian.	Pentadbir ICT, Pengurus ICT dan ICTSO

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CDO	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer*

GLOSARI	
	Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.

GLOSARI	
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Sistem informasi	Sistem informasi termasuk sistem operasi, infrastruktur, *business applications*, *off-the-shelf products*, perkhidmatan dan aplikasi yang dibangunkan.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

	PKPMP-BTM-ISMS-P1-001-B001 **LAMPIRAN 1** **SURAT AKUAN PEMATUHAN** **DASAR KESELAMATAN ICT PKPMP**

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT PKPMP

Nama :…….
Jawatan :…….
Jabatan / Bahagian :…….

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya berjanji bahawa saya akan mematuhi peruntukan Dasar Keselamatan ICT Pejabat Ketua Pendaftar Mahkamah Persekutuan Malaysia serta apa-apa peraturan dan arahan lain yang berkaitan dikeluarkan dan dikuatkuasakan dari masa ke semasa selanjutnya tempoh perkhidmatan saya.

2. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub di dalam Dasar Keselamatan ICT Jabatan; dan

3. Jika saya ingkar kepada peruntukan–peruntukan yang ditetapkan dan disabitkan kerana melanggar Dasar Keselamatan ICT Jabatan, maka tindakan tatatertib boleh diambil ke atas diri saya mengikut Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib 1993).

……..

(Tandatangan Pegawai / Kakitangan)

Tarikh: ……

Disahkan Oleh:

Pegawai Keselamatan ICT (ICTSO)

……
( )

Tarikh: ……..

Diperakukan Oleh :

Ketua Pegawai Digital (CDO)

……
( )

Tarikh: ……..

	PKPMP-BTM-ISMS-P1-001-B002 **LAMPIRAN 2** **SURAT AKUAN PEMATUHAN** **DASAR KESELAMATAN ICT PKPMP** **(PEMBEKAL)**

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT PKPMP (PEMBEKAL)

Nama :……
Jawatan :……
Syarikat :……

Adalah saya _____, nombor kad pengenalan _____ yang mewakili Syarikat _____,No Pendaftaran _____ dengan ini mengaku bahawa perhatian saya telah ditarik kepada Dasar Keselamatan ICT Pejabat Ketua Pendaftar Mahkamah Persekutuan Malaysia dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam dasar tersebut.

Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub di dalam Dasar Keselamatan ICT; dan

Sekiranya saya atau mana-mana individu yang mewakili syarikat ini didapati melanggar dasar yang telah ditetapkan, maka saya sebagai wakil syarikat bersetuju tindakan undang-undang boleh diambil ke atas sesiapa yang terlibat mengikut peruntukan-peruntukan undang-undang sedia ada yang sedang berkuatkuasa.

……..
(Tandatangan)
Tarikh: ……

Disahkan Oleh:	**Diperakukan Oleh :**
Pegawai Keselamatan ICT (ICTSO)	**Ketua Pegawai Digital (CDO)**
……	……
( )	( )
Tarikh: ……..	Tarikh: ……

	PKPMP-BTM-ISMS-P1-001-B003 **LAMPIRAN 3** **PERAKUAN AKTA RAHSIA RASMI 1972 (KONTRAKTOR)**

Perakuan Untuk Ditandatangani Oleh Kontraktor Berkenaan Dengan Akta Rasmi 1972

Adalah saya dengan ini mengaku bahawa perhatian saya telah dirujuk kepada peruntuk-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkah laku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya peroleh dalam

Pejabat Ketua Pendaftar Mahkamah Persekutuan

adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas melaksanakan :

……..……..……..……

……..……..……..……

……..……..……..……

Tandatangan : ……..
Nama : Cop Syarikat:
No. Kad Pengenalan :
Jawatan :
Syarikat :
Tarikh :

Disaksikan oleh : ……
(Tandatangan)
Nama : Cop Jabatan:
No. Kad Pengenalan :
Jawatan :
Tarikh :

	PKPMP-BTM-ISMS-P1-001-B004 **LAMPIRAN 4** **PENGECUALIAN PEMATUHAN DASAR KESELAMATAN ICT PKPMP**

Pemohon	
Nama	
Tarikh	
Unit & Bahagian	
Tarikh Mula Pengecualian	
Tarikh Akhir Pengecualian	
Butiran & Justifikasi Pengecualian	
Tandatangan Pemohon: Tarikh:	Disahkan Oleh: Tarikh:

Diluluskan Oleh ICTSO / Pengarah BTM
Tandatangan: Nama: Jawatan & Cop Rasmi: Tarikh:

	PKPMP-BTM-ISMS-P1-001-B005 **LAMPIRAN 5** **SENARAI PERUNDANGAN DAN PERATURAN**

SENARAI PERUNDANGAN DAN PERATURAN

1. Akta Mahkamah Rendah 1948 (Akta 92);
2. Akta Kaedah-Kaedah Mahkamah Rendah 1955 (Disemak 1971) (Akta 55);
3. Akta Mahkamah Kehakiman 1964 (Akta 91);
4. Kanun Prosedur Jenayah (CPC) (Akta 593);
5. Kaedah-kaedah Mahkamah Persekutuan 1995 (PU(A) 376/1995);
6. Kaedah-kaedah Mahkamah Rayuan 1994 (PU(A) 524/1994);
7. Kaedah-kaedah Mahkamah Tinggi 1980 (PU(A) 50/1980);
8. Kaedah-kaedah Mahkamah Rendah 1980 (PU(A) 328/1980);
9. Pekeliling Ketua Pendaftar/Timbalan Ketua Pendaftar;
10. Pekeliling Pendaftar Mahkamah Tinggi Malaya/Sabah dan Sarawak;
11. Pekeliling Pendaftar Mahkamah Rayuan;
12. Arahan Amalan Ketua Hakim Negara;
13. Arahan Amalan Hakim Besar Malaya dan Hakim Besar Sabah dan Sarawak;
14. Surat Arahan Ketua Pendaftar Tahun 2010 Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di PKPMP;
15. Arahan Keselamatan;
16. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
17. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002;
18. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
19. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
20. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
21. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
22. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
23. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
24. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

	PKPMP-BTM-ISMS-P1-001-B005 **LAMPIRAN 5** **SENARAI PERUNDANGAN DAN PERATURAN**

25. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
26. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
27. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
28. Akta Tandatangan Digital 1997 (Akta 562);
29. Akta Rahsia Rasmi 1972 (Akta 88) ;
30. Akta Jenayah Komputer 1997 (Akta 563);
31. Akta Komunikasi dan Multimedia 1998 (Akta 588);
32. Perintah-Perintah Am;
33. Arahan Perbendaharaan;
34. Arahan Teknologi Maklumat 2007;
35. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
36. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
37. Akta-akta/ Kaedah/ Pekeliling/ Arahan lain yang berkaitan.
38. *Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control);*
39. Akta Arkib Negara 2003;
40. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh;
41. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (*espionage*);
42. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976; Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Ketua Pengarah Negara Melalui Surat M(R)10308/3/(45) Bertarikh 8 Mei 1987; dan
43. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R) 200/ 55 Klt.7 (21) Bertarikh 21 Ogos 1999.
44. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959;
45. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan;
46. *State Key Points;*

	PKPMP-BTM-ISMS-P1-001-B005 **LAMPIRAN 5** **SENARAI PERUNDANGAN DAN PERATURAN**

47. Surat Pekeliling Am Rahsia Bil.1 Tahun 1975 - Keselamatan Jabatan-jabatan Kerajaan;
48. Surat Bil. KPKK/308/A (2) bertarikh 7/9/79 - Mencetak Pas-Pas Keselamatan dan Kad-Kad Pengenalan PKPMPM;
49. Surat Pekeliling Am Bil 4 Tahun 1982 - Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan
50. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.
51. *Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidential;*
52. *General Circular Memorandum;*
53. *Instruction On Positive Vetting Procedure;*
54. Surat Pekeliling Am Sulit Bil.1/1966 – Perkara Keselamatan Tentang Persidangan-Persidangan/ Perjumpaan/Lawatan Sambil Belajar Antarabangsa;
55. Surat Pekeliling Tahun 1966 – Tapisan Keselamatan Terhadap Pakar/Penasihat Luar Negeri;
56. Surat Pekeliling Am Sulit Bil.1/1967 – Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka-mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam Perwakilan Rasmi Malaysia semasa melawat Negara-negara Tabir Buluh dan Tabir besi;
57. Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 - Melaporkan Perjumpaan/ Percakapan Di Antara Diplomat/ Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota-Anggota Kerajaan; dan
58. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.
59. Akta Hak Cipta (Pindaan) 1997;
60. Akta Multimedia dan Telekomunikasi 1998;
61. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;
62. Akta Pencegahan Dan Pengawalan Penyakit Berjangkit 1988
63. Peraturan-Peraturan Pencegahan Dan Pengawalan Penyakit Berjangkit (Pengkompaunan Kesalahan-Kesalahan) (Pindaan) (No.7) 2020;
64. Peraturan-Peraturan Pencegahan Dan Pengawalan Penyakit Berjangkit (Langkah-Langkah Di Dalam Kawasan Tempatan Jangkitan) (No.7) 2020.
65. Akta dan Peraturan-peraturan lain yang berkaitan.