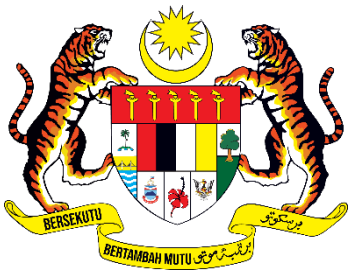

POLISI KESELAMATAN SIBER PKPMP

PEJABAT KETUA PENDAFTAR
MAHKAMAH PERSEKUTUAN MALAYSIA

Versi Dokumen: 1.0
Nombor Dokumen: PKPMP-BTM-ISMS-P1-001

	PKPMP-BTM-ISMS-P1-001 **POLISI KESELAMATAN SIBER PKPMP**

A. INFORMASI DOKUMEN

Jenis Dokumen: Manual Keselamatan	**Nombor Dokumen:** PKPMP-BTM-ISMS-P1-001	**Rujukan Fail:** PKPMP-100-15/1/1
	Versi Dokumen: 1.0	**Tarikh Berkuatkuasa:** 27/04/2025
Disediakan Oleh: Yusri Hakim bin Yeop (Penolong Pengarah Kanan BTM) Tarikh: 20/01/2025	**Disemak Oleh:** Mohamad Khairi bin Kareem (Pengarah BTM) Tarikh: 24/03/2025	**Diluluskan Oleh:** Azhaniz Teh bin Azman Teh (Timbalan Ketua Pendaftar) Tarikh: 27/03/2025
Pengedaran Dokumen: BTM		

	PKPMP-BTM-ISMS-P1-001 **POLISI KESELAMATAN SIBER PKPMP**

B. REKOD PINDAAN

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
1.0	27/03/2025	Salinan Pertama Pindaan Dasar Keselamatan ICT PKPMP v 4.0 (DKICT) kepada Polisi Keselamatan Siber merujuk Standard ISO/IEC 27001:2022.	Keseluruhan Dokumen	Timbalan Ketua Pendaftar

ISI KANDUNGAN

1.0 PENGENALAN

1.1 Polisi Keselamatan Siber (PKS) Pejabat Ketua Pendaftar Mahkamah Persekutuan Malaysia (PKPMP) adalah dokumen yang menetapkan prosedur dan panduan yang jelas dalam usaha memastikan keselamatan maklumat secara komprehensif. Polisi ini telah mendapat kelulusan rasmi dan komitmen penuh daripada pengurusan tertinggi untuk pelaksanaan yang efektif.

1.2 PKS PKPMP dibangunkan untuk mewujudkan rangka kerja yang komprehensif dalam melindungi aset maklumat PKPMP daripada ancaman dan kerentanan yang berkemungkinan timbul. Polisi ini disediakan sebagai panduan untuk melindungi kerahsiaan, integriti dan ketersediaan maklumat serta mematuhi keperluan undang-undang dan peraturan yang relevan di PKPMP merangkumi arahan, peraturan, garis panduan dan amalan yang ditetapkan serta data yang sensitif dan kritikal daripada capaian yang tidak sah, kehilangan atau pendedahan yang tidak dibenarkan.

1.3 PKS PKPMP ini mentakrifkan kawalan keselamatan yang sesuai berdasarkan dasar, pekeliling dan garis panduan Kerajaan semasa yang berkuat kuasa serta amalan terbaik keselamatan yang relevan. Polisi ini terpakai kepada semua sistem dan persekitaran maklumat PKPMP untuk memastikan perlindungan menyeluruh terhadap ancaman siber yang semakin kompleks.

1.4 PKS PKPMP disediakan supaya pengurusan keselamatan data dan maklumat PKPMP lebih efisien dan efektif serta boleh meningkatkan tahap perlindungan keselamatan ke tahap yang lebih tinggi.

2.0 OBJEKTIF

2.1 Objektif utama PKS PKPMP adalah seperti yang berikut:

a) Melindungi kepentingan pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dalam aspek kerahsiaan, integriti, ketersediaan dan kesahihan maklumat serta penyangkalan ;

b) Mematuhi keperluan perundangan, peraturan, standard, pekeliling dan prosedur yang sedang berkuat kuasa.

c) Melaksanakan pengurusan risiko dan insiden keselamatan siber yang lebih berkesan.

d) Memastikan penyampaian perkhidmatan PKPMP pada tahap keselamatan tertinggi yang boleh meningkatkan keyakinan pihak berkepentingan seperti Kerajaan, industri dan orang awam.

e) Menjamin kelancaran operasi dan kesinambungan perkhidmatan PKPMP dengan meminimumkan impak insiden keselamatan maklumat fizikal dan logikal.

f) Mencegah penyalahgunaan atau kecurian maklumat Kerajaan.

g) Meminimumkan kerosakan, kemusnahan dan kos sekiranya berlaku kegagalan dan ancaman.

h) Menyediakan asas untuk penambahbaikan yang berterusan dalam pengurusan keselamatan dan pentadbiran teknologi maklumat dan komunikasi.

3.0 SKOP

3.1 PKS PKPMP adalah panduan utama untuk semua warga PKPMP dan pihak-pihak yang terlibat dalam pengurusan data atau maklumat. Polisi ini menggariskan tanggungjawab, peranan, arahan, peraturan, garis panduan dan amalan yang **WAJIB DIBACA**, **DIFAHAMI** dan **DIPATUHI** oleh semua warga PKPMP termasuk pembekal, perunding dan pihak-pihak yang terlibat dengan perkhidmatan teknologi maklumat dan komunikasi PKPMP.

3.2 Polisi ini juga terpakai untuk melindungi semua aset maklumat PKPMP. Aset maklumat ini termasuk data dan maklumat dalam bentuk digital (*softcopy*) atau bercetak (*hardcopy*), perkakasan, perisian, infrastruktur ICT, manusia dan premis. Aset ini adalah penting dan berharga untuk memastikan PKPMP dapat menjalankan tugas rasmi Kerajaan dengan lancar kepada masyarakat, sektor swasta dan jabatan Kerajaan yang berkaitan.

3.3 PKS PKPMP menetapkan keperluan asas adalah seperti yang berikut:

a) Kebolehcapaian Data dan Maklumat

Data dan maklumat hendaklah boleh dicapai secara berterusan dengan pantas, tepat, mudah dan boleh dipercayai. Ini adalah penting untuk memastikan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

b) Kerahsiaan dan Kesempurnaan Maklumat

Semua data dan maklumat hendaklah dilindungi kerahsiaannya dan dikendalikan dengan baik pada setiap masa untuk memastikan ketepatan dan melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat.

c) Penghapusan Rekod dan Teknik Penyamaran Data

Kaedah penghapusan rekod dan teknik penyamaran data yang selamat hendaklah mengikut prosedur keselamatan yang berkuatkuasa bagi mengelakkan pendedahan data sensitif dari akses yang tidak dibenarkan.

3.4 Bagi menentukan sistem ICT ini terjamin keselamatannya sepanjang masa, PKS PKPMP merangkumi perlindungan semua bentuk maklumat Kerajaan yang diwujudkan, diproses, disimpan, dihantar, dijana, dicetak, diakses, diedarkan, diselenggara, dihapuskan, dimusnahkan dan dibuat salinan serta diarkibkan dalam persekitaran ICT PKPMP. Perlindungan ini dilaksanakan melalui sistem kawalan dan prosedur pengendalian yang menyeluruh bagi elemen-elemen seperti yang berikut:

a) Data atau Maklumat

Koleksi fakta dalam bentuk kertas atau mesej elektronik yang mengandungi maklumat yang boleh digunakan untuk mencapai objektif dan misi PKPMP. Contohnya, sistem dokumentasi, prosedur operasi, rekod, profil warga PKPMP, profil pelanggan, profil kontraktor, pangkalan data, fail data, maklumat arkib dan sebagainya.

b) Peralatan ICT

Semua peralatan berkomputer seperli komputer peribadi, komputer riba, peripheral seperti sebuah komputer, stesen kerja (*workstation*), kerangka utama (*mainframe*), peranti keselamatan rangkaian, peranti rangkaian dan peralatan sokongan IT seperti *Uninterrupted Power Supply* (UPS); *Power Distribution Unit* (PDU); dan *Environment Monitoring System* (EMS).

c) Infrastruktur ICT

Set lengkap perkakasan, perisian, rangkaian dan kemudahan yang menyokong pemprosesan, penyimpanan dan penghantaran maklumat dalam organisasi termasuk *Local Area Network* (LAN), *Wide Area Network* (WAN), sistem kad akses dan perkhidmatan pengkomputeran awan serta kemudahan sokongan seperti bekalan elektrik dan sistem pencegah kebakaran.

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) Salinan Digital (*Softcopy*)

Fakta dalam bentuk digital yang digunakan untuk mencapai objektif dan misi PKPMP termasuk rekod digital, pangkalan data dan maklumat arkib.

f) Salinan Bercetak (*Hardcopy*)

Fakta dalam bentuk bercetak seperti sistem dokumentasi, prosedur operasi, rekod dan fail.

g) Perkakasan (*Hardware*)

Semua aset yang digunakan untuk menyokong penyediaan, pemprosesan dan kemudahan storan maklumat PKPMP. Contohnya, komputer, pelayan (*server*), peralatan komunikasi, PABX dan sebagainya.

h) Perisian (*Software*)

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contohnya, perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat.

i) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop tugas harian bagi mencapai misi dan objektif PKPMP. Individu berkenaan merupakan aset berdasarkan kepada tugas dan fungsi yang dilaksanakan.

j) Premis Komputer dan Komunikasi

Semua kemudahan dan premis yang digunakan untuk menempatkan eleman di atas hendaklah diberikan perlindungan yang rapi untuk mencegah kebocoran maklumat rahsia atau kelemahan perlindungan yang akan dianggap sebagai perlanggaran kepada peraturan keselamatan.

3.5 Polisi ini memastikan bahawa setiap elemen di atas diberikan perlindungan yang sewajarnya untuk meminimumkan risiko dan mengekalkan integriti operasi PKPMP.

4.0 PERNYATAAN POLISI KESELAMATAN SIBER PKPMP

4.1 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.

4.2 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.

5.0 PRINSIP KESELAMATAN DATA DAN MAKLUMAT

5.1 Prinsip keselamatan data dan maklumat yang menjadi asas kepada PKS PKPMP dan perlu dipatuhi adalah seperti yang berikut:

a) Capaian Atas Dasar Perlu Mengetahui

Capaian terhadap penggunaan aset maklumat hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Ini bermakna capaian hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk capaian adalah berdasarkan klasifikasi dan peringkat dokumen seperti yang dinyatakan dalam Arahan Keselamatan (Semakan dan Pindaan 2017) perenggan 53, muka surat 15.

b) Hak Capaian Minimum

Pengguna hendaklah diberikan hak capaian minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak capaian pengguna hanya diberikan pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan capaian adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses atau capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan sahaja mengikut peranan dalam fungsi tugasan masing-masing dan kebenaran untuk melaksanakan operasi tertentu berdasarkan peranan tersebut. Hak capaian hendaklah dikaji dari semasa ke semasa atau sekurang-kurangnya sekali dalam tempoh setahun

berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

c) Capaian Akses Administrator

Capaian Akses Administrator merujuk kepada hak istimewa (*privileged access*) yang diberikan kepada individu tertentu dalam organisasi untuk mengurus dan mengawal sistem, rangkaian, aplikasi, serta pangkalan data. Akses ini membolehkan pengguna melakukan tindakan yang tidak boleh dilakukan oleh pengguna biasa, seperti memasang perisian, mengubah tetapan sistem, mengurus akaun pengguna lain, dan mengakses data sensitif.

Oleh kerana capaian ini berisiko tinggi, ia perlu dikawal dengan ketat bagi mengelakkan penyalahgunaan atau serangan siber yang boleh menyebabkan kebocoran data, pemusnahan sistem, atau eksploitasi infrastruktur IT.

d) Akauntabiliti

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

i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.

ii) Memeriksa dan menentukan data dan maklumat tepat dan lengkap dari semasa ke semasa.

iii) Menentukan maklumat sedia untuk digunakan.

iv) Menjaga kerahsiaan kata laluan.

v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.

vi) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.

vii) Menjaga kerahsiaan langkah-langkah keselamatan maklumat dari diketahui umum.

e) Pengasingan Tugas

PKPMP hendaklah melaksanakan pengasingan tugas bagi tugasan yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya untuk mengekalkan prinsip semak-dan-imbang (*check-and-balance*).

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset

maklumat daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan tugas juga merangkumi tindakan memisahkan antara kumpulan pembangunan aplikasi, operasi, rangkaian dan keselamatan mengikut kesesuaian.

f) Prinsip Kepercayaan Sifar (*Zero Trust*)

Prinsip ini menegaskan bahawa tiada pengguna, peranti atau rangkaian harus dipercayai secara automatik sama ada berada dalam atau luar perimeter rangkaian. Setiap permintaan untuk mencapai data atau maklumat hendaklah melalui proses pengesahan yang teliti sebelum diberikan hak capaian. Prinsip ini menyatakan bahawa:

i) Semua trafik rangkaian dalaman dan luaran dianggap sebagai tidak dipercayai.

ii) Capaian kepada sumber diberikan berdasarkan set kriteria yang komprehensif dan dinamik termasuk identiti pengguna, keadaan dan kesihatan peranti, lokasi capaian serta faktor konteks lain yang relevan. Capaian kepada sumber hanya akan diluluskan selepas pengesahan menyeluruh terhadap identiti pengguna dan status peranti tanpa mengira lokasi fizikal untuk memastikan keselamatan yang maksimum.

iii) Capaian kepada sumber diberikan berdasarkan keperluan semasa dan tempoh masa yang ditetapkan.

g) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti tahap pematuhan terhadap PKS bagi mengawal insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan kesediaan aset maklumat memelihara semua rekod berkaitan tindakan keselamatan. Tujuannya adalah untuk memastikan bahawa aktiviti tersebut mematuhi peraturan piawaian dan prosedur yang ditetapkan serta mengidentifikasi isu, ketidakpatuhan dan potensi risiko. Oleh itu, aset maklumat seperti komputer, pelayan (*server*), penghala rangkaian (*network router*), tembok keselamatan (*firewall*) dan peralatan rangkaian hendaklah dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit.

h) Pematuhan

PKS PKPMP hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan Maklumat.

i) Pemulihan

Pemulihan sistem selepas berlaku gangguan atau kegagalan diperlukan untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk memulihkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penyalinan semula penduaan (*restore backup*) dan mewujudkan pelan pemulihan bencana atau kesinambungan perkhidmatan.

j) Saling Bergantungan

Setiap prinsip keselamatan adalah saling ~~lengkap-~~melengkapi dan bergantung antara satu sama lain untuk membentuk sistem keselamatan yang menyeluruh dan berkesan. Prinsip-prinsip ini tidak boleh dilaksanakan secara terpisah tetapi hendaklah diintegrasikan dan diselaraskan untuk mencapai keselamatan yang maksimum.

6.0 CIRI KESELAMATAN DATA DAN MAKLUMAT

6.1 PKS PKPMP melindungi semua jenis maklumat elektronik bertujuan untuk menjamin keselamatan data dan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan data dan maklumat adalah seperti yang berikut:

a) Kerahsiaan

Kerahsiaan merujuk kepada perlindungan maklumat daripada capaian yang tidak dibenarkan. Ciri keselamatan ini bertujuan untuk memastikan hanya pihak yang diberi kuasa dan dibenarkan sahaja boleh mencapai maklumat tertentu. Perkara ini penting untuk melindungi maklumat sensitif seperti data peribadi, maklumat kewangan dan rahsia perniagaan. Langkah-langkah yang biasa digunakan untuk mengekalkan kerahsiaan termasuk penyulitan maklumat, kawalan capaian yang ketat dan penggunaan kata laluan yang kukuh.

b) Integriti

Integriti merujuk kepada ketepatan, kelengkapan dan kesempurnaan maklumat. Ciri keselamatan ini bertujuan untuk memastikan data dan maklumat tidak diubah suai atau dirosakkan oleh pihak yang tidak dibenarkan. Sebarang perubahan terhadap data dan maklumat hendaklah dilakukan hanya oleh pihak yang mempunyai kebenaran yang sah dan perubahan tersebut haruslah direkodkan dengan jelas untuk tujuan audit. Integriti sangat penting dalam memastikan bahawa keputusan yang dibuat berdasarkan maklumat tersebut adalah tepat dan boleh dipercayai.

c) Tidak Boleh Disangkal

Punca data dan maklumat yang tidak boleh disangkal merujuk kepada perkara yang sah dan multak. Ciri keselamatan ini bertujuan untuk memastikan pihak yang bertanggungjawab terhadap penciptaan, penghantaran atau penerimaan data dan maklumat tidak boleh menafikan penglibatan mereka. Dalam transaksi digital, ciri keselamatan ini dapat membuktikan penglibatan pihak tertentu dalam transaksi secara digital yang dilaksanakan. Sebagai contohnya, langkah keselamatan yang digunakan untuk memastikan tiada penafian termasuk penggunaan tandatangan digital dan rekod transaksi yang terperinci semasa jejak audit.

d) Kesahihan

Kesahihan merujuk kepada pengesahan data dan maklumat adalah sah dan berasal daripada sumber yang dipercayai. Ciri keselamatan ini bertujuan untuk memastikan maklumat yang diterima atau dihantar tidak dimanipulasi oleh pihak ketiga. Langkah-langkah seperti penggunaan sijil digital dan protokol pengesahan membantu memastikan bahawa maklumat yang diterima adalah sahih dan boleh dipercayai.

e) Ketersediaan

Ketersediaan merujuk kepada data dan maklumat boleh dicapai oleh pihak yang yang dibenarkan pada bila-bila masa yang diperlukan. Ciri keselamatan ini bertujuan untuk memastikan kelancaran operasi harian dan membuat keputusan yang tepat pada masanya. Untuk mengekalkan ketersediaan, semua pihak yang terlibat hendaklah melaksanakan langkah-langkah seperti menyediakan dan pengaktifan pelan pemulihan bencana, menyediakan sistem sandaran dan melaksanakan pengurusan risiko yang komprehensif untuk meminimumkan gangguan terhadap capaian data dan maklumat.

7.0 IMPLIKASI KETIDAKPATUHAN POLISI KESELAMATAN SIBER

7.1 Ketidakpatuhan terhadap PKS PKPMP boleh mengakibatkan pelbagai implikasi yang serius termasuk tetapi tidak terhad kepada:

a) Risiko Keselamatan

Ketidakpatuhan boleh membawa kepada pendedahan data sensitif, pencerobohan sistem atau gangguan operasi yang mengakibatkan kehilangan data dan maklumat penting atau kerosakan kepada infrastruktur digital.

b) Gangguan Operasi

Ketidakpatuhan boleh menganggu operasi harian termasuk gangguan sistem, kehilangan data dan kerosakan peralatan yang menjejaskan penyampaian perkhidmatan secara langsung.

c) Kesan Undang-Undang

Kegagalan untuk mematuhi polisi ini boleh membawa kepada tindakan undang-undang terhadap individu yang terlibat termasuk denda atau tindakan undang-undang lain yang berkaitan dengan pelanggaran peraturan dan undang-undang keselamatan siber.

d) Kerugian Kewangan

Ketidakpatuhan boleh membawa kepada kerugian kewangan yang besar, sama ada melalui denda, kos pemulihan atau kehilangan kepercayaan pelanggan dan pihak berkepentingan yang menjejaskan kedudukan kewangan PKPMP.

e) Kerosakan Reputasi

Insiden keselamatan siber yang disebabkan oleh ketidakpatuhan boleh membawa kepada merosakkan reputasi PKPMP, mengurangkan kepercayaan pihak berkepentingan dan masyarakat umum terhadap keupayaan PKPMP untuk mengawal keselamatan siber.

f) Tindakan Disiplin

Warga PKPMP yang gagal mematuhi PKS ini boleh dikenakan tindakan tatatertib termasuk amaran, penggantungan atau penamatan perkhidmatan, bergantung kepada tahap pelanggaran yang dilakukan.

8.0 PENGURUSAN RISIKO KESELAMATAN MAKLUMAT

8.1 Semua pihak yang terlibat dalam pengurusan data dan maklumat di PKPMP hendaklah mengambil kira risiko yang wujud terhadap aset maklumat berikutan kerentanan (*vulnerability*) dan ancaman yang semakin meningkat dalam persekitaran digital masa kini. Oleh itu, PKPMP hendaklah mengambil langkah proaktif dan bersesuaian untuk menilai tahap risiko terhadap aset maklumat bagi memastikan pendekatan dan keputusan yang paling berkesan dapat dikenal pasti dalam menyediakan perlindungan dan kawalan yang optimum.

8.2 Penilaian risiko ini bertujuan untuk mengenal pasti dan melaksanakan tindakan susulan dan *mitigate* yang sesuai untuk mengurangkan atau mengawal risiko keselamatan maklumat berdasarkan keputusan penilaian risiko. Penilaian risiko keselamatan maklumat hendaklah dilaksanakan secara berkala **sekurang-kurangnya sekali setahun** atau sekiranya terdapat perubahan pada aset maklumat.

8.3 Penilaian risiko keselamatan maklumat hendaklah dilaksanakan pada semua aset maklumat PKPMP termasuk aset fizikal, aplikasi, perisian, pelayan (*server*) dan rangkaian serta proses dan prosedur yang berkaitan. Penilaian risiko ini juga hendaklah dilaksanakan di premis yang menempatkan aset maklumat seperti pusat data, bilik media storan, kemudahan utility dan sistem sokongan lain.

8.4 Pelaksanaan pengurusan risiko hendaklah selaras dengan Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024. Dalam menghadapi potensi risiko, semua pihak yang terlibat perlu mengenal pasti tindakan yang sewajarnya, termasuk:

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian.

b) Menerima atau bersedia untuk menghadapi risiko yang mungkin berlaku, selagi risiko itu tidak menjejaskan penyampaian perkhidmatan PKPMP.

c) Mengelak atau mencegah risiko dengan mengambil tindakan yang boleh mengelakkan atau mencegah berlakunya risiko.

Mengambil tindakan yang boleh mengelakkan atau mencegah terjadinya risiko.

d) Memindahkan risiko kepada pihak ketiga seperti pembekal, pakar runding atau pihak berkepentingan lain.

9.0 PENGECUALIAN KRITERIA

9.1 Permohonan pengecualian PKS dan prosedur ICT boleh dibuat dengan melengkapkan borang Pengecualian Pematuhan Polisi Keselamatan Siber 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.

10.0 TEKNOLOGI

10.1 Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data di setiap elemen pengkomputeran seperti yang berikut:

10.1.1 Peringkat Pemprosesan Data

a) Data-dalam-simpanan (*Data-at-rest*)

i) PKPMP hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan

dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.

ii) Maklumat Rahsia Rasmi, Maklumat Rasmi dan Personally Identifiable Information (PII) perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

b) Data-dalam-pergerakan (*Data-in-motion*)

i) PKPMP hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-pergerakan.

c) Data-dalam-penggunaan (*Data-in-use*)

i) PKPMP hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih

berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

ii) Teknologi yang bersesuaian boleh digunakan oleh PKPMP untuk memastikan asal data dan data/transaksi tanpa sangkal.

d) Perlindungan Ketirisan Data (*Data Leakage Protection*)

i) Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

ii) Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

10.1.2 Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, PKPMP hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (*counter measure dan control measure*) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan (Semakan dan Pindaan 2017) yang dikeluarkan oleh Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan dari CGSO.

Setiap projek ICT hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan seperti di bawah:

a) Peranti Pengkomputeran Peribadi

i) Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja (*workstation*), telefon pintar, tablet dan peranti storan.

ii) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada PKPMP. Peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

b) Peranti Rangkaian

i) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suiz rangkaian (m*switch)*, penghala Rangkaian (*router*), tembok

keselamatan (*firewall*), peranti *Virtual Private Network* (VPN) dan kabel.

ii) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data.

c) Perisian Aplikasi

i) Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi dan sistem operasi.

ii) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam- simpanan dan menghalang ketirisan data.

d) Pelayan

i) Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

ii) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk mellindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.

e) Persekitaran Fizikal

i) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

ii) Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip kawalan *defence-in-depth*.

iii) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.

11.0 PROSES

11.1 PKPMP hendaklah melindungi keselamatan ICT dengan melaksanakan perkara-perkara berikut:

11.1.1 Konfigurasi Asas

a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan.

b) Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

11.1.2 Kawalan Perubahan Konfigurasi

a) Prosedur kawalan perubahan konfigurasi hendaklah diwujudkan dan dilaksanakan bagi perubahan kepada sistem, termasuk tampalan perisian (*system patches*), pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

b) Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh Pegawai Keselamatan ICT (ICTSO) yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.

c) ICTSO yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

11.1.3 Sandaran

a) Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa untuk memastikan bahawa proses kerja boleh dilaksanakan.

b) Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

11.1.4 Kitaran Pengurusan Aset

a) Pindah (Pekeliling Perbendaharaan AM2.6 Pindahan)

i) Memindahkan hak miik Aset Alih antara Pusat Tanggungjawab (PTJ) agensi Kerajaan Persekuturan dengan PTJ agensi Kerajaan Persekutuan yang lain.

ii) Pemindahan hak milik aset berlaku dalam keadaan berikut (lebih kepada penggunan dan pemulangan):

a) Warga PKPMP meninggalkan agensi disebabkan oleh persaraan, peletakan jawatan atau penugasan semula.

b) Aset yang dikongsi untuk kegunaan sementara.

c) Pemberian aset kepada agensi lain.

d) Aset dikembalikan setelah tamat tempoh sewaan.
e) Mewujudkan pangkalan data yang baru oleh pemilik baru.
f) Memudahkan pengesahan dan pemantauan.
g) Membolehkan pemilik baru mengguna pakai aset alih tersebut.

b) Pindah
i) Pemindahan hak milik aset berlaku dalam keadaan berikut:
a) Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (c).

c) Pelupusan
i) Pelupusan aset ICT perlu merujuk kepada Pekeliling Perbendaharaan AM 2.7 (Pelupusan Aset Tak Alih), AM 7.7 (Pelupusan Aset Tak Ketara) dan PKPMP-PK (S)-27 Pengurusan Aset Alih PKPMP.
ii) Pelupusan dalam bentuk pemusnahan fizikal pada media storan tersebut.
iii) Pelupusan dalam bentuk sanitasi data (*sanitizing*), iaitu proses pembersihan data pada media storan menggunakan kaedah yang diiktiraf seperti *data wiping*, *degaussing*, atau *secure erasure* bagi memastikan data tidak boleh dipulihkan semula.

d) Kitaran Hayat

i) Kitaran hayat data hendaklah diuruskan mengikut Akta 629 atau mengikut keperluan PKPMP.

ii) Akta 629 memaklumkan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

iii) Umumnya, terdapat empat (4) fasa utama yang dilalui oleh sesuatu aset dalam tempoh hayatnya:

a) Fasa **Perancangan** Aset: Keperluan untuk aset baru dikenal pasti dirancang dan disediakan.

b) Fasa **Pewujudan** Aset: Aset tersebut diwujudkan dan dimiliki melalui proses pewujudan yang ditetapkan.

c) Fasa **Penggunaan** Aset: Aset digunakan, beroperasi dan disenggarakan.

d) Fasa **Pelupusan** Aset: Penggunaan aset dihentikan apabila perkhidmatan tidak diperlukan lagi atau hilang atau tidak ekonomi digunakan.

12.0 MANUSIA

12.1 Warga PKPMP, pembekal dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

12.2 Sistem penyampaian perkhidmatan PKPMP hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan pengguna hendaklah dibangunkan bagi semua warga PKPMP.

12.2.1 Kompetensi Pengguna

a) Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan ICT dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan ICT.

b) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga PKPMP berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

c) Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah disarankan.

12.2.2 Kompetensi Pelaksana

a) Warga PKPMP yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

b) ICTSO hendaklah memenuhi syarat-syarat berikut:

i) Pegawai yang dilantik oleh Pengurusan PKPMP.

ii) Memenuhi keperluan pembelajaran berterusan.

iii) Menimba pengalaman yang mencukupi dalam bidang keselamatan ICT.

iv) Memperoleh tapisan keselamatan daripada agensi yang diberi kuasa.

c) ICTSO yang dilantik oleh PKPMP hendaklah memenuhi keperluan kompetensi di atas. ICTSO bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di PKPMP.

12.2.3 Peranan Pengguna

d) Peranan pengguna hendaklah diberi berdasarkan keperluan dan bidang tugas pengguna.

e) Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani dokumen [*Non-Disclosure Agreement* (NDA)] seperti Arahan Keselamatan (Semakan dan Pindaan 2017). Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

f) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.

g) Warga PKPMP yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT PKPMP dikembalikan sekiranya berlaku perubahan peranan.

h) Warga PKPMP yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset PKPMP yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.

i) Warga PKPMP lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset PKPMP dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh PKPMP

1. BIDANG 01 KAWALAN ORGANISASI

0101 Polisi Keselamatan Siber

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PKPMP dan perundangan yang berkaitan.

010101 Pelaksanaan Polisi Keselamatan Maklumat	Tanggungjawab
Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan PKPMP kepada warga PKPMP, pengguna, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di PKPMP. Ketua Pendaftar PKPMP selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) PKPMP adalah bertanggungjawab terhadap pelaksanaan polisi ini dengan dibantu oleh JPICT PKPMP. Ahli JPICT ini terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Pengarah Bahagian Teknologi Maklumat, Pengarah Mahkamah Negeri, semua Ketua Bahagian dan ahli-ahli yang dilantik oleh Ketua Pendaftar PKPMP. PKS perlu menangani keperluan: Strategik PKPMP. Peraturan, undang-undang dan kontrak. Ancaman semasa dan akan datang terhadap persekitaran keselamatan maklumat.	Ketua Pendaftar

PKS hendaklah mengandungi kenyataan yang membabitkan: a) Definisi keselamatan maklumat, objektif dan prinsip kepada semua aktiviti yang berhubung dengan keselamatan maklumat. Tanggungjawab am dan khusus bagi pengurusan keselamatan maklumat. Proses ketidakpatuhan pengendalian dan pengecualian keselamatan maklumat. Kajian semula dasar keselamatan PKPMP perlu menilai peluang untuk penambahbaikan dasar sebagai tindak balas kepada perubahan persekitaran organisasi, keadaan perniagaan dan keadaan undang-undang.	
010102 Penguatkuasaan Polisi	**Tanggungjawab**
PKS PKPMP mestilah dipatuhi oleh semua warga PKPMP, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di PKPMP. Sebarang ketidakpatuhan kepada polisi ini boleh mengakibatkan tindakan tatatertib termasuk sebarang tindakan undang-undang lain di bawah akta/peraturan/ undang-undang semasa yang berkuat kuasa.	Warga PKPMP, pembekal, perunding dan pihak-pihak
010103 Pengecualian Polisi	**Tanggungjawab**
Polisi ini terpakai kepada warga PKPMP dan pembekal serta semua pihak yang terlibat dalam pembekalan perkhidatan ICT di PKPMP dan tiada pengecualian diberikan.	Warga PKPMP, pembekal dan pihak-pihak
010104 Penyelenggaraan Polisi	**Tanggungjawab**

Penyelenggaraan dan kajian semula dasar hendaklah dilaksanakan mengikut diperlukan. Semua dokumen atau rekod hendaklah diwujudkan dan diselenggara untuk menyediakan bukti pematuhan kepada keperluan dan operasi berkesan pengurusan keselamatan maklumat. Semua dokumen dan rekod hendaklah dilindungi dan dikawal mengikut undang-undang/arahan/peraturan/garis panduan semasa yang berkuat kuasa.	JPICT dan ICTSO
010105 Kajian Semula Dan Semakan Polisi Keselamatan Siber	**Tanggungjawab**
Polisi ini hendaklah disemak dan dikemas kini secara berkala mengikut jangka masa yang ditetapkan atau serta-merta apabila berlaku perubahan ketara dalam teknologi, aplikasi, prosedur, perundangan, atau polisi Kerajaan. Langkah ini adalah kritikal bagi memastikan polisi kekal relevan, mencukupi, dan berkesan dalam melindungi kepentingan organisasi serta menjamin keselamatan data dan maklumat. Berikut ialah prosedur yang berkaitan dengan kajian semula PKS: a) Memastikan penguatkuasaan pelaksanaan PKS PKPMP ini direkodkan. b) Mengenal pasti dan menentukan perubahan yang diperlukan.	Ketua Pendaftar / Pegawai yang diturunkan kuasa

c) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada JPICT/Ketua Pendaftar PKPMP bagi tujuan kelulusan. d) Memaklumkan pindaan yang telah diluluskan oleh JPICT kepada warga PKPMPserta semua pihak yang terlibat dalam perkhidmatan ICT di PKPMP. e) Polisi ini hendaklah dikaji semula setiap tiga (3) tahun atau mengikut keperluan semasa sekiranya perubahan tersebut kurang dari tempoh kajian semula bagi memastikan dokumen sentiasa relevan.	

0102 Peranan Dan Tanggungjawab Dalam Keselamatan Maklumat	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PKPMP.	
010201 Ketua Pendaftar	**Tanggungjawab**
Peranan dan tanggungjawab Ketua Pendaftar adalah seperti yang berikut: a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber. b) Merangka, mengkaji semula pelaksanaan dan keberkesanan PKS mengikut keperluan. c) Memberi arahan dan hala tuju yang jelas serta sokongan pengurusan yang mantap. d) Mewujudkan dan mengetuai Jawatankuasa Pemandu Keselamatan ICT PKPMP.	Ketua Pendaftar

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 PKS PKPMP. g) Memastikan semua pengguna mematuhi PKS 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 PKS PKPMP. j) Menandatangani "Surat Akuan Pematuhan" bagi mematuhi PKS. Sila rujuk Lampiran 1.	
010202 Ketua Pegawai Digital (CDO)	**Tanggungjawab**
Peranan dan tanggungjawab CDO yang dilantik adalah seperti yang berikut: a) Membaca, memahami dan mematuhi PKS. 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 PKS PKPMP. g) Memastikan dan melaksanakan program-program kesedaran mengenai keselamatan ICT. h) Menyelia dan memantau perlaksanaan PKS di peringkat negeri. i) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar PKS PKPMP. j) Menandatangani "Surat Akuan Pematuhan" bagi mematuhi PKS. Sila rujuk Lampiran 1.	
010203 Pengurus ICT	**Tanggungjawab**
Pengarah, Bahagian Teknologi Maklumat (BTM) merupakan Pengurus ICT PKPMP. Peranan dan tanggungjawab Pengurus ICT adalah seperti yang berikut: a) Membaca, memahami dan mematuhi PKS 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 ancaman 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.	Pengarah BTM

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 PKS PKPMP kepada ICTSO. k) Menyelaraskan program-program kesedaran mengenai keselamatan ICT.	
010204 Pegawai Keselamatan ICT (ICTSO)	**Tanggungjawab**
a) Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti yang berikut: b) Membaca, memahami dan mematuhi Polisi Keselamatan Siber Kerajaan. c) Menguatkuasakan PKS PKPMP. d) Mengurus keseluruhan program-program keselamatan ICT PKPMP. e) Memberi penerangan dan pendedahan berkenaan PKS PKPMP kepada semua pengguna. f) Menjalankan penilaian risiko. g) Menyelaraskan program audit, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya. h) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi	ICTSO

khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian. i) Melaporkan insiden keselamatan ICT kepada Pasukan Tindakbalas Insiden Keselamatan ICT (GCERT-NACSA) dan memaklumkannya kepada Ketua Jabatan, CDO dan Pengurus ICT. j) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera.	
010205 Pentadbir Sistem ICT	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti yang berikut: a) Membaca, memahami dan mematuhi PKS 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 Polisi Keselamatan Siber 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. h) Menyimpan dan menganalisis rekod jejak audit.	Pentadbir Sistem ICT: a.Pentadbir Pusat Data; b.Pentadbir E-mel; c.Pentadbir Rangkaian; d.Pentadbir Sistem dan Aplikasi e. Pentadbir Aset dan Sumber ICT

010206 Pengguna PKPMP	Tanggungjawab
a) Peranan dan tanggungjawab pengguna adalah seperti yang berikut: b) Membaca, memahami dan mematuhi PKS PKPMP. c) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya. d) Menjaga kerahsiaan maklumat Kerajaan yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. e) Menjaga kerahsiaan kata laluan. f) Menukar kata laluan mengikut tempoh yang ditetapkan dalam PKS ICT atau serta-merta apabila diarahkan bagi memastikan keselamatan akses ke sistem dan maklumat terpelihara. g) Memastikan maklumat berkaitan adalah tepat dan lengkap dari semasa ke semasa. h) Mengambil bahagian dalam program-program kesedaran mengenai keselamatan ICT (sama ada secara langsung atau tidak langsung). i) Menandatangani “Surat Akuan Pematuhan” bagi mematuhi PKS PKPMP. Sila rujuk Lampiran 1.	Pengguna
010207 Pengguna Luar	**Tanggungjawab**
Terdiri daripada pembekal, pakar runding dan pihak-pihak yang berkepentingan. Peranan dan tanggungjawab pengguna luar adalah seperti yang berikut: a) Membaca, memahami dan mematuhi PKS PKPMP.	Penguna Luar

b) Menjaga kerahsiaan kata laluan yang diberikan. c) Menggunakan kemudahan ICT dengan berpandukan garis panduan yang telah ditetapkan. d) Menandatangani Surat Akuan Pematuhan PKS PKPMP (Lampiran 2) dan Borang Akta Rahsia Rasmi (Lampiran 3).	
010208 Jawatankuasa Pemandu ICT PKPMP	**Tanggungjawab**
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. f) Meluluskan dan mengesahkan PKS.	JPICT
010209 Pasukan Projek ISMS PKPMP	**Tanggungjawab**
Projek Persijilan ISO/IEC 27001:2022 dilaksanakan oleh sebuah pasukan projek yang terdiri dari pegawai-pegawai yang dilantik. 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.	Pasukan Projek ISMS

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. j) Merancang pelan latihan, kompetensi dan kesedaran ISMS.	
010210 Computer Security Incident Response Team (CSIRT) PKPMP	**Tanggungjawab**
Keanggotaan CSIRT adalah seperti yang berikut: Pengerusi: CDO Ahli : ICTSO : Pegawai Teknologi Maklumat Penolong Pegawai Teknologi Maklumat Peranan dan tanggungjawab CSRIT adalah seperti yang berikut: a) **Menerima, menganalisis, dan merekod insiden keselamatan ICT** yang dilaporkan oleh pengguna atau sistem pemantauan. b) **Menilai tahap kritikal insiden** dan mengambil tindakan mitigasi segera untuk mengawal impak. c) **Menyelaras dan melaksanakan tindak balas insiden** mengikut prosedur yang ditetapkan, termasuk tindakan pemulihan awal.	CSIRT PKPMP

d) **Melapor insiden kritikal kepada pihak berkaitan** seperti *National Cyber Coordination and Command Center* (**NC4) NACSA, Ketua Jabatan, dan Pengurus ICT** untuk tindakan selanjutnya. e) **Menjalankan siasatan asas terhadap punca insiden** dan mencadangkan langkah pembaikan bagi mengelakkan kejadian berulang. f) **Menyediakan laporan ringkas pasca insiden** untuk dokumentasi dan rujukan masa hadapan.	
010211 Audit Dalaman/Pihak Ketiga PKPMP	**Tanggungjawab**
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. e) Menjalankan audit susulan bagi mengesahkan tindakan pembetulan yang dilaksanakan. f) Mengemukakan Laporan Audit Susulan kepada Jawatankuasa Pemandu ISMS.	Pasukan Audit ISMS
0103 Pengasingan Tugas Dan Tanggungjawab	
Objektif: Mengurangkan risiko penipuan, kesilapan dan pemintasan dalam kawalan keselamatan maklumat.	

010301 Keperluan Keselamatan Dalam Pengasingan Tugas	Tanggungjawab
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset ICT. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT. b) Tugas mewujud, memadam, mengemas kini, mengubah atau mengesah data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. c) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	Ketua Jabatan/ Bahagian/ Seksyen

0104 Tanggungjawab Pengurusan
Objektif: Memastikan pengurusan memahami peranan dalam keselamatan maklumat dan mengambil tindakan yang bertujuan untuk memastikan semua kakitangan menyedari dan memenuhi tanggungjawab dalam keselamatan maklumat PKPMP.

010401 Tanggungjawab Pengurusan Terhadap Pengguna	Tanggungjawab
Perkara yang perlu dipatuhi termasuk yang berikut: a) Pengurusan ICT PKPMP hendaklah memastikan semua pegawai dan kakitangan PKPMP serta pengguna luar mematuhi PKS 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 dan Pengguna Luar

0105 Hubungan Dengan Pihak Berkuasa	
Objektif: Memastikan aliran maklumat berkaitan keselamatan berlaku dengan sewajarnya di antara PKPMP dan pihak berkuasa.	
010501 Hubungan Dengan Pihak Berkuasa	**Tanggungjawab**
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara yang perlu dipatuhi termasuk yang berikut: a) Mewujudkan dan mengemas kini senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. b) Pihak berkuasa perundangan ialah NACSA, Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM). Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba.	CSIRT PKPMP

c) Mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab PKPMP. d) Menandatangani "Surat Akuan Pematuhan" bagi mematuhi PKS. Sila rujuk Lampiran 1.	

0106 Hubungan Dengan Pihak Berkepentingan Yang Khusus

Objektif:

Memastikan aliran maklumat berkaitan keselamatan berlaku dengan sewajarnya.

010601 Hubungan Dengan Pihak Berkepentingan Yang Khusus	**Tanggungjawab**
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan seperti *Malaysia Cybersecurity Community Rawsec, Cyber Security Malaysia (CSM)* dan pertubuhan profesional hendaklah dikekalkan. Keperluan hubungan dengan pihak berkepentingan yang khusus adalah seperti yang berikut: a) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat. b) Memastikan pemahaman tentang persekitaran keselamatan maklumat adalah terkini. c) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini. d) Mendapat capaian kepada nasihat pakar keselamatan maklumat. e) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan.	Pengurus ICT

f) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	

0107 Risikan Ancaman (*Threat Intelligence*)

Objektif:

Menyediakan pemahaman yang mendalam mengenai ancaman keselamatan siber yang berpotensi memberi impak kepada organisasi dengan mengumpul, menganalisis, dan menyebarkan maklumat ancaman bagi membolehkan tindakan mitigasi yang proaktif dan berkesan diambil.

010701 Risikan Ancaman (Threat Intelligence)	**Tanggungjawab**
Maklumat ancaman keselamatan yang berpotensi menjejaskan fungsi PKPMP perlu diperoleh dan dianalisis bagi menghasilkan perisikan berkaitan. Maklumat tentang ancaman sedia ada atau baharu akan dikumpul dan dianalisis untuk memudahkan tindakan dan mengelakkan ancaman atau mengurangkan impak kepada aset maklumat yang terlibat. Pemilik aset maklumat hendaklah melaksanakan tindakan berikut bagi meningkatkan tahap kawalan keselamatan aset: a) Mengenal pasti ancaman dengan melaksanakan penilaian risiko terhadap aset maklumat. b) Mengenal pasti dan melaksanakan kawalan keselamatan yang berkaitan. Kawalan keselamatan tersebut juga dijadikan sebagai satu daripada keperluan dalam kitar hayat pembangunan sistem dan penyediaan infrastruktur ICT.	ICTSO

c) Maklumat ancaman keselamatan perlu diambil kira sebagai faktor utama dalam pelaksanaan ujian keselamatan bagi sistem dan infrastruktur ICT, berdasarkan analisis risikan ancaman yang diperoleh.	

0108 Keselamatan Maklumat Dalam Pengurusan Projek

Objektif:

Memastikan risiko keselamatan maklumat berkaitan projek dan serahan ditangani dengan berkesan dalam pengurusan projek sepanjang kitaran hayat projek.

010801 Keselamatan Maklumat Dalam Pengurusan Projek	**Tanggungjawab**
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek tanpa mengira kerumitan, saiz, tempoh dan bidang. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek PKPMP. b) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek. c) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan. d) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS PKPMP. e) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal mempunyai pensijilan keselamatan maklumat.	Ketua Pendaftar

f) Kesesuaian pertimbangan dan aktiviti keselamatan maklumat hendaklah disusuli pada peringkat yang telah ditetapkan seperti jawatankuasa teknikal projek atau jawatankuasa pemandu projek g) Peranan dan tanggungjawab keselamatan maklumat projek hendaklah ditakrifkan dan ditentukan.	
010802 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat (Information Security Requirements Analysis and Specifications)	**Tanggungjawab**
Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada serta mematuhi perkara seperti yang berikut: a) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pembentukan konsep perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan. b) Semua sistem yang dibangunkan sama ada secara dalaman atau khidmat luar hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan PKS PKPMP. c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan. d) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data. Penilaian Tahap Keselamatan (*Security Posture Assessment*, SPA) hendaklah dilaksanakan	Pentadbir Sistem ICT

sebelum sistem digunakan dalam persekitaran produksi. Pelaksanaan hendaklah mematuhi Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024. e) Ujian hendaklah dilakukan oleh syarikat yang mempunyai lesen Penyedia Perkhidmatan Keselamatan Siber (*Licensing of Cyber Security Service Provider*) yang sah dari NACSA.	

0109 Pengurusan Aset ICT

Objektif:

Untuk mengenal pasti aset bagi memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT PKPMP.

010901 Inventori Aset	**Tanggungjawab**
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.	Pengguna PKPMP & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos

d) Memastikan pengendalian, pelupusan dan pemusnahan aset dikendalikan mengikut prosedur yang ditetapkan. e) Semakan inventori ke atas aset ICT dan kemudahan pemprosesan maklumat perlu dilakukan sekurang-kurangnya sekali setahun.	
010902 Hak Milik Aset	**Tanggungjawab**
Aset hak milik PKPMP hendaklah diselenggara mengikut jadual penyelenggaraan yang ditetapkan serta mematuhi Pekeliling Perbendaharaan Malaysia Am 1.1 Pengurusan Aset Kerajaan.Tanggungjawab yang perlu dipatuhi oleh pemilik aset merangkumi perkara seperti yang berikut: a) Memastikan aset didaftarkan dalam senarai aset mengikut klasifikasi aset dan diserahkan kepada pemilik aset. b) Memastikan semua jenis aset dipelihara dan diselenggara dengan baik. c) Kenal pasti dan kaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan. d) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapuskan atau dilupuskan. e) Aset bukan hakmilik PKPMP termasuklah aset sewaan hendaklah didaftarkan dan diurus mengikut prosedur/arahan-arahan atau polisi *Bring Your Own Device* (BYOD) yang sedang berkuat kuasa.	Pengguna PKPMP & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos

010903 Pengelasan Maklmat Aset	Tanggungjawab
Memastikan setiap maklumat dalam aset ICT dikelaskan mengikut klasifikasi dan peringkat keselamatan dokumen selaras dengan Akta Rahsia Rasmi 1972.	Pegawai Aset

0110 Penggunaan Maklumat Dan Aset ICT

Objektif:

Memastikan maklumat dan aset ICT dilindungi, diguna dan dikendali sewajarnya.

011001 Penerimaan Penggunaan Aset	Tanggungjawab
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. Prosedur bagi mengendalikan aset hendaklah dibangunkan dan dilaksanakan mengikut kerangka 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.	Pengguna PKPMP & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos

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. g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

0111 Pemulangan Aset ICT

Objektif:

Melindungi aset PKPMP sebagai sebahagian dari proses pertukaran atau penamatan perkhidmatan kakitangan, kontrak dan perjanjian.

011101 Pemulangan Aset ICT	**Tanggungjawab**
Pengguna perlu mengembalikan aset termasuk semua aset lain yang berkaitan seperti peranti storan mudah alih, peranti pengguna fizikal yang disambungkan kepada sistem rangkaian, salinan maklumat fizikal dan perkakasan pengesahan (contohnya kunci mekanikal, token fizikal dan kad pintar) untuk sistem maklumat, tapak serta arkib fizikal mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan atau penamatan perkhidmatan atau kontrak. Pemulangan aset yang mengandungi maklumat rasmi kerajaan hendaklah disanitasi mengikut Surat Pekeliling Am Bilangan 4 Tahun 2022 Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam.	Pengguna PKPMP & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos

0112 Pengelasan Maklumat

	PKPMP-BTM-ISMS-P1-001 **POLISI KESELAMATAN SIBER PKPMP**

Objektif:

Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian selaras dengan kepentingan organisasi.

011201 Pengelasan Maklumat	**Tanggungjawab**
Data dan maklumat perlu dikelas oleh Pegawai Pengelas mengikut keperluan keselamatan maklumat yang telah ditetapkan dalam Arahan Keselamatan berdasarkan keperluan perlindungan keselamatan makluamt tersebut. Pengkelasan maklumat terdiri daripada aktiviti penentuan klasifikasi maklumat serta penentuan peringkat keselamatan maklumat. Klasifikasi maklumat terdiri daripada maklumat rahsia rasmi dan maklumat rasmi manakala peringkat keselamatan maklumat terdiri daripada rahsia besar, rahsia, sulit terhad, data terkawal/sensitif dan terbuka. Perkara di bawah hendaklah dilaksanakan oleh semua pihak yang terlibat dalam pengkelasan maklumat: a) Maklumat hendaklah dikelaskan Pegawai Pengelas yang dilantik oleh PKPMP dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan dalam Arahan Keselamatan. b) Mematuhi piawaian, prosedur, tatacara dan garis panduan keselamatan dan pengendalian maklumat atau dokumen yang sedang berkuat kuasa. c) Memberi perhatian semasa mengendalikan maklumat rahsia terperingkat. d) Memastikan tiada pendedahan maklumat kepada pihak yang tidak dibenarkan.	Ketua Pendaftar, CDO dan Pegawai ICT

e) Pengelasan maklumat hendaklah berpandukan kepada Akta Rahsia Rasmi 1972, Arahan Keselamatan, Pekeliling Am Bilangan 2 Tahun 1987 - Garis Panduan Mengenai \ Fail. f) Pengurusan maklumat dan rekod hendaklah berpandukan kepada Akta Arkib Negara 2003, Pekeliling Am Bilangan 5 Tahun 2007 - Pengurusan Rekod Awam, Arahan Keselamatan dan standard berkaitan pengurusan rekod serta pekeliling, arahan, dasar dan garis panduan yang dikeluarkan oleh Pejabat Pegawai Keselamatan Kerajaan dan Arkib Negara Malaysia. g) Memastikan kesemua fail fizikal dan digital maklumat disimpan mengikut keperluan perlindungan keselamatan yang ditetapkan oleh pihak Kerajaan.	

0113 Pelabelan Maklumat	
Objektif: Memudahkan komunikasi dalam pengelasan maklumat dan menyokong automasi pemprosesan dan pengurusan maklumat.	
011301 Pelabelan Maklumat	**Tanggungjawab**
Peringkat keselamatan maklumat hendaklah ditandakan mengikut klasifikasi dokumen yang kekal terjilid dengan huruf cerai atau huruf besar tidak kurang daripada 7mm di sebelah luar kulit hadapan dan belakang, di muka tajuk, di muka surat pertama dan penghabisan. Peringkat keselamatan maklumat hendaklah diletakkan pada penjuru sebelah atas kiri dan sebelah bawah kanan	Ketua Pendaftar, CDO dan Pegawai ICT

dan setiap muka surat yang mengandungi perkara bertulis, bercetak atau bercap. Semua maklumat yang ditandakan sebagai terperingkat hendaklah mematuhi Arahan Keselamatan: Keselamatan Rahsia Rasmi dan semua maklumat yang diklasifikasikan terperingkat dalam format elektronik hendaklah mematuhi Arahan Keselamatan: Keselamatan Rahsia Rasmi Dalam Persekitaran Teknologi Maklumat dan Komunikasi (ICT).	

0114 Pertukaran Maklumat

Objektif:

Memastikan keselamatan perpindahan/pertukaran maklumat dan perisian antara PKPMP dan pihak luar terjamin.

011401 Polisi Dan Prosedur Pemindahan Maklumat	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Polisi, 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. d) Memastikan maklumat yang terdapat dalam e-mel hendaklah dilindungi sebaik-baiknya.	Semua Pengguna, Pentadbir Rangkaian, Pentadbir Emel dan ICTSO

011402 Perjanjian Mengenai Pemindahan Maklumat	Tanggungjawab
PKPMP perlu mengambil kira keselamatan maklumat organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara PKPMP dengan pihak luar serta mematuhi Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional. Perkara yang perlu dipertimbangkan adalah: a) Pengarah Bahagian hendaklah mengawal penghantaran dan penerimaan data atau maklumat jabatan. b) Mewujudkan prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat jabatan. c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat. d) Mengenal pasti perlindungan data dalam penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.	CDO dan Pengurus ICT
011403 Pengurusan Mel Elektronik (E-mel)	**Tanggungjawab**
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 yang berikut: a) **Penggunaan Akaun E-Mel**	Semua Pengguna

- Hanya **akaun e-mel rasmi PKPMP** yang dibenarkan untuk urusan rasmi.
- **Dilarang** menggunakan akaun milik individu lain atau akaun yang dikongsi bersama.

Format E-Mel

- Setiap e-mel yang dihantar hendaklah mengikut format rasmi yang telah ditetapkan oleh PKPMP.

Subjek dan Kandungan E-Mel

- Pastikan subjek dan kandungan e-mel berkaitan dengan perkara perbincangan sebelum penghantaran dilakukan.

Ketepatan Alamat Penerima

- Gunakan akaun e-mel rasmi untuk penghantaran e-mel rasmi.
- Semak dan pastikan alamat e-mel penerima adalah betul sebelum menghantar e-mel.

Penghantaran Lampiran (Fail Kepilan)

- Pengguna dinaskan menggunakan fail kepilan tidak melebihi dua puluh (20) MB semasa penghantaran.
- Penggunaan kaedah pemampatan untuk mengurangkan saiz fail adalah disarankan.

Penghantaran Fail Berskala Besar

- Fail yang melebihi dua puluh (20) MB hendaklah dihantar melalui pautan muat turun (URL) dengan memastikan ciri-ciri keselamatan dilaksanakan.

Keselamatan E-Mel

- Jangan buka e-mel daripada penghantar yang tidak diketahui atau mencurigakan.

- Kenal pasti dan sahkan identiti penghantar sebelum meneruskan transaksi maklumat melalui e-mel.
- Pengguna hendaklah peka terhadap e-mel amaran yang dihantar oleh pentadbir e-mel berkaitan ancaman keselamatan, percubaan phishing, atau arahan keselamatan lain.
- Pengguna juga hendaklah sentiasa peka terhadap mesej daripada sistem e-mel berkaitan keperluan menukar kata laluan setiap tiga ratus (300) hari dan mengambil tindakan segera untuk menukarnya bagi memastikan keselamatan akaun.

Pengurusan Rekod E-Mel

- Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan.
- E-mel yang tidak penting, telah diambil tindakan, dan tidak mempunyai nilai arkib boleh dihapuskan.

Ketepatan Tarikh dan Masa

- Pastikan tarikh dan masa sistem komputer adalah tepat bagi memastikan keabsahan rekod komunikasi.

Tindak Balas Terhadap E-Mel

- Beri maklum balas terhadap e-mel dengan segera dan ambil tindakan sewajarnya.

Larangan Penggunaan E-Mel Peribadi

- Akaun e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my) tidak boleh digunakan untuk tujuan rasmi.

Penyelenggaraan Akaun E-Mel • Setiap pengguna bertanggungjawab ke atas penyelenggaraan peti masuk (mailbox) masing-masing bagi memastikan kelancaran komunikasi rasmi.	

0115 Kawalan Capaian

Objektif:

Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.

011501 Polisi Kawalan Capaian	**Tanggungjawab**
Polisi khusus mengenai kawalan capaian hendaklah ditakrifkan dengan mengambil kira keperluan ini dan harus dimaklumkan kepada semua pihak yang berkepentingan yang berkaitan. Pemilik maklumat dan Pemilik Aset hendaklah menentukan tahap perlindungan keselamatan maklumat dan kawalan capaian yang diperlukan bagi mencapai maklumat tersebut. Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Kawalan capaian ditetapkan berdasarkan prinsip perlu tahu iatu capaian diberikan atas dasar keperluan untuk melaksanakan tugas dan keperluan untuk digunakan iaitu hanya diberikan capaian kepada infrastruktur teknologi maklumat di mana terdapat keperluan yang jelas.	ICTSO, Pengurus ICT dan Pentadbir ICT

Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Kawalan capaian perlu disemak, dikemas kini dan disahkan sekurang-kurangnya sekali dalam tempoh setahun atau mengikut keperluan sekiranya terdapat perubahan serta menyokong peraturan kawalan capaian pengguna sedia ada.

Perkara yang perlu dipatuhi adalah seperti yang 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 privileged.

011502 Capaian Kepada Rangkaian Dan Perkhidmatan Rangkaian	Tanggungjawab
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. b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian. c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Pengurus ICT dan Pentadbir Rangkaian

0116 Pengurusan Identiti	
Objektif: Membenarkan individu dan sistem yang menggunakan identiti unik membuat capaian kepada maklumat PKPMP dan aset ICT serta melaksanakan tugasan berdasarkan hak capaian.	
011601 Pendaftaran Pengguna, Pertukaran Pengguna dan Pembatalan Pengguna	**Tanggungjawab**
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian. Proses pendaftaran dan pembatalan pengguna hendak disemak dan dikemaskini sekurang-kurangnya satu (1) kali setahun. Perkara-perkara berikut hendaklah dipatuhi:	Pengguna PKPMP & Pengguna Luar, Pentadbir ICT, Pengurus ICT dan ICTSO

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.

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 memperakukan ciri-ciri kata laluan yang lebih baik kepada pengguna. iii) Menghalang kemasukan maklumat dari laman Internet yang berunsur ganas, lucah, permainan elektronik atas talian, judi dan lain-lain aktiviti yang dilarang.	

0117 Pengesahan Maklumat

Objektif:

Memastikan pengesahan entiti yang betul dan mengelakkan kegagalan ketika proses pengesahan.

011701 Pengurusan Kata Laluan Pengguna	**Tanggungjawab**
a) Peruntukan kata laluan perlu melalui beberapa proses pengurusan formal. b) Pengguna perlu menandatangani kenyataan untuk menyimpan kata laluan dan untuk menjaga authentikasi kerahsiaan kumpulan (iaitu password yang dikongsi bersama); kenyataan yang ditandatangani boleh dimasukkan dalam terma-terma dan syarat-syarat pekerjaan. c) Pengguna perlu disediakan dengan kata laluan sementara yang pengguna perlu menukar kata laluan pada penggunaan pertama. d) Prosedur perlu diwujudkan untuk mengesahkan identiti pengguna sebelum menyediakan kata laluan yang baru, penggantian atau sementara.	Pengguna PKPMP dan Pengguna Luar, Pentadbir ICT, Pengurus ICT dan ICTSO

e) Kata laluan sementara perlu diedar kepada pengguna dengan selamat dimana katalaluan tidak boleh diedarkan oleh pihak ketiga dan dalam *clear text*. f) Kata laluan sementara yang dicipta hendaklah unik dan susah dianggar. g) Pengguna perlu mengesahkan penerimaan kata laluan. h) Kata laluan vendor default perlu diubah selepas pemasangan sistem atau perisian.	

0118 Hak Capaian	
Objektif: Memastikan kawalan capaian oleh pengguna yang dibenarkan sahaja.	
011801 Semakan Capaian Pengguna (*Provisioning*)	**Tanggungjawab**
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
011802 Kajian Semula Hak Capaian Pengguna	**Tanggungjawab**
Pentadbir aset hendaklah menyemak hak capaian pengguna secara berkala sekurang-kurangnya satu (1) kali dalam tempoh setahun atau sekiranya terdapat perubahan atau keperluan. Pentadbir Sistem perlu mewujudkan rekod pendaftaran dan penamatan pengguna sistem masing-masing sebagai rujukan semakan ke atas hak capaian pengguna secara berkala. Semakan ke atas hak capaian fizikal dan logik harus mempertimbangkan perkara berikut:	Pentadbir ICT, Pengurus ICT dan ICTSO

a) Hak capaian pengguna selepas sebarang perubahan dalam organisasi (contohnya pertukaran pekerjaan, kenaikan pangkat, penurunan pangkat) atau penamatan perkhidmatan/pekerjaan. b) Kebenaran untuk hak capaian Istimewa.	
011803 Pembatalan atau Pelarasan Hak Capaian	**Tanggungjawab**
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 sertta 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
0119 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	
Objektif: Memastikan perlindungan aset PKPMP yang boleh diakses oleh pembekal.	
011901 Dasar Keselamatan Maklumat Untuk Pembekal	**Tanggungjawab**
Keperluan keselamatan maklumat hendaklah ditakrifkan, dilaksanakan, dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset PKPMP. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:	BTM dan Pembekal

a) Mengenal pasti dan mendokumentasi maklumat pembekal. b) Menyediakan prosedur pengurusan pembekal termasuk kaedah penilaian mutu perkhidmatan. c) Memilih pembekal mengikut klasifikasi maklumat dan perkhidmatan yang disediakan oleh pembekal selaras dengan dasar dan peraturan yang berkuat kuasa. d) Mengawal dan memantau capaian pembekal. e) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam dokumen perjanjian. f) Jenis-jenis obligasi kepada pembekal. g) Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat. h) Melaksanakan program kesedaran terhadap PKS PKPMP kepada pembekal. i) Menandatangani Surat Akuan Pembida Berjaya dan Surat Setuju Terima. j) Pembekal perlu mematuhi arahan keselamatan yang sedang berkuat kuasa. k) Mengenal pasti dan melaksanakan proses dan prosedur bagi mengurus risiko yang berkaitan dengan penggunaan produk dan perkhidmatan pembekal termasuk penamatan penggunaan produk dan perkhidmatan pembekal. l) Menandatangani Surat Akuan Pematuhan PKS PKPMP (LAMPIRAN A).	

Pemilik perkhidmatan atau projek hendaklah memastikan proses penamatan pembekal yang selamat, termasuk: a) Membatalkan peruntukan hak capaian. b) Pengendalian maklumat. c) Menentukan pemilikan harta intelek yang dibangunkan semasa penjanjian dilaksanakan. d) Mudah alih maklumat sekiranya berlaku pertukaran pembekal atau penyumberan. e) Pengurusan rekod. f) Pemulangan aset. g) Pelupusan selamat maklumat dan aset lain yang berkaitan. h) Keperluan kerahsiaan berterusan.	

0120 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam hubungan pembekal.	
012001 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal	**Tanggungjawab**
Semua keperluan keselamatan maklumat hendaklah relevan dan dipersetujui dengan setiap pembekal bagi mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur, maklumat organisasi IT. Perkara yang perlu diambil kira adalah seperti yang 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.	BTM dan Pembekal

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.

Semua keperluan keselamatan maklumat yang berkaitan hendaklah ditakrifkan, disediakan dan dipersetujui dengan setiap pembekal yang boleh mencapai, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi.

Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak jabatan selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.

Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Syarikat pembekal hendaklah mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam kod bidang yang berkaitan.

b) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan.

c) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada jabatan berkaitan.

d) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi.

e) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal.

f) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut:

   i) Badan penilai pihak ketiga adalah bebas dan berintegriti.

   ii) Badan penilai pihak ketiga adalah kompeten.

   iii) Kriteria penilaian.

   iv) Parameter pengujian.

   v) Andaian yang dibuat berkaitan dengan skop penilaian.

g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mencapai, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk

keperluan jabatan bagi perjanjian kerahsiaan atau ketakdedahan maklumat dan Perakuan Akta Rahsia Rasmi 1972 (Akta 88). h) Pembekal hendaklah mematuhi pengkelasan maklumat yang telah ditetapkan oleh PKPMP.	

0121 Pengurusan Keselamatan Maklumat Dalam Rantaian Bekalan Teknologi Maklumat Dan Komunikasi	
Objektif: Mengekalkan tahap persetujuan bagi keselamatan maklumat dalam hubungan pembekal.	
012101 Kawalan Rantaian Bekalan Maklumat Dan Komunikasi	**Tanggungjawab**
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan maklumat dan komunikasi. Perkara yang perlu diambil kira adalah seperti yang 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.	BTM dan Pembekal

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	

0122 Pengurusan Pemantauan, Kajian Semula Dan Perubahan Perkhidmatan Pembekal

Objektif:

Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan penyampaian perkhidmatan adalah sama seperti perjanjian pembekal.

012201 Pemantauan dan Kajian Semula Perkhidmatan Pembekal	**Tanggungjawab**
PKPMP hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal. Perkara yang perlu diambil kira adalah seperti yang 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

012202 Pengurusan Perubahan Perkhidmatan Pembekal	**Tanggungjawab**
Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diurus dengan mengambil kira kepentingan maklumat, sistem dan perkhidmatan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut: a) Perubahan dalam perjanjian dengan 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.	BTM dan Pembekal
0123 Perkhidmatan Pengkomputeran Awan (*Cloud Services*)	
Objektif: Menentukan dan mengurus keselamatan maklumat dalam penggunaan perkhidmatan *cloud*.	
012301 Keselamatan Maklumat Bagi Penggunaan Perkhidmatan Pengkomputeran Awan (*Cloud Services*)	**Tanggungjawab**
Pengurusan perkhidmatan awan ini melibatkan pelbagai aspek teknikal dan pentadbiran untuk memastikan perkhidmatan awan digunakan secara berkesan, selamat, dan sesuai dengan keperluan organisasi. Perkara berikut perlu dipatuhi adalah seperti yang berikut:	Pengguna dan Pembekal

a) Memastikan kepatuhan terhadap keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak yang berkaitan antaranya:
   i) PK 2.6: Perolehan Perkhidmatan Pengkomputeran Awan (*Cloud*) Sektor Awam.
   ii) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam.
   iii) Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan dalam Perkhidmatan Awam.
   iv) Pengurusan perkhidmatan yang disediakan oleh pembekal yang dilantik oleh pihak Kerajaan.
   v) Menentukan/mentakrifkan dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan.
   vi) Memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan.
   vii) Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.

Elemen pengkomputeran awan adalah seperti yang berikut:

a) 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*.

b) 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.

c) Keselamatan Operasi Pentadbir

Prosedur untuk operasi pentadbiran persekitaran pengkomputeran *cloud* harus ditakrifkan, didokumenkan dan dipantau.

d) Pemantauan Untuk Perkhidmatan *Cloud*

Pengguna perkhidmatan *cloud* harus mempunyai keupayaan untuk memantau aspek tertentu operasi perkhidmatan *cloud* yang digunakan oleh pengguna perkhidmatan *cloud*.

e) 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.	

0124 Pengurusan Dan Penambahbaikan Insiden Keselamatan Maklumat

Objektif:

Memastikan insiden keselamatan maklumat dikendalikan dengan pantas, sistematik, dan berkesan bagi meminimumkan impak, mengenal pasti saluran komunikasi yang tepat, serta mengesan dan menangani kelemahan yang menyebabkan insiden.

012401 Tanggungjawab Dan Prosedur	**Tanggungjawab**
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat dengan mentakrif, mewujudkan dan menyampaikan proses pengurusan insiden keselamatan maklumat, peranan dan tanggungjawab. Pengurusan insiden PKPMP ialah berdasarkan prosedur pengurusan pengendalian insiden keselamatan maklumat yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Melaksanakan program kesedaran mengenai prosedur pengendalian insiden keselamatan dan hebahan kepada warga PKPMP. b) Memastikan personel yang mengurus insiden mempunyai tahap kompetensi yang diperlukan. Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi	ICTSO, Pengurus ICT dan CERT PKPMP

tentang kejadian dan kerentanan kelemahan keselamatan.	

0125 Penilaian Dan Keputusan Mengenai Aktiviti Keselamatan Maklumat

Objektif:

Memastikan kategori dan keutamaan yang efektif dalam kejadian keselamatan maklumat.

012501 Penilaian Dan Keputusan Mengenai Aktiviti Keselamatan Maklumat	**Tanggungjawab**
Aktiviti keselamatan maklumat hendaklah dinilai dan diputuskan sama ada untuk diklasifikasikan sebagai insiden keselamatan maklumat berdasarkan pekeliling dan prosedur pengurusan insiden keselamatan maklumat yang sedang berkuat kuasa.	ICTSO dan BTM

0126 Tindak Balas Terhadap Insiden Keselamatan Maklumat

Objektif:

Memastikan tindak balas yang efisien dan efektif kepada insiden keselamatan maklumat.

012601 Pengurusan Maklumat Insiden Keselamatan ICT	**Tanggungjawab**
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah ditetapkan bagi memastikan pengurusan insiden yang sistematik dan berkesan. Beberapa kawalan utama yang perlu diambil kira dalam proses pengumpulan maklumat dan pengurusan insiden adalah seperti berikut: **A. Tindakan Segera Semasa Insiden** a) **Mengumpulkan bukti** secepat mungkin selepas insiden keselamatan berlaku.	ICTSO, BTM dan CERT PKPMP

b) **Menjalankan kajian forensik**, sekiranya diperlukan, untuk mengenal pasti punca insiden.

c) **Menghubungi pihak berkaitan** dengan segera bagi mendapatkan bantuan atau pengesahan.

d) **Menyimpan jejak audit dan sandaran secara berkala**, serta memastikan integriti semua bahan bukti terpelihara.

e) **Menyalin bahan bukti** dan merekodkan semua aktiviti berkaitan dengan proses penyalinan.

f) **Mengaktifkan pelan kontingensi** dan memastikan kesinambungan perkhidmatan bagi mengurangkan gangguan operasi.

g) **Melaksanakan tindakan pemulihan segera** bagi menangani insiden dengan pantas.

h) **Memaklumkan atau mendapatkan nasihat daripada pihak berkuasa berkaitan**, sekiranya diperlukan.

B. Tindakan Selepas Insiden

a) **Menutup insiden secara rasmi** dan merekodkan semua butiran selepas insiden berjaya dikendalikan.

b) **Melaksanakan analisis pasca-kejadian** untuk mengenal pasti punca asal insiden dan mendokumentasikan dapatan mengikut prosedur yang ditetapkan.

c) **Mengenal pasti dan mengurus kelemahan keselamatan maklumat**, termasuk kegagalan kawalan keselamatan yang menyumbang atau gagal mencegah insiden.

0127 Pengalaman Dari Insiden Keselamatan Maklumat	
Objektif: Mengurangkan kebarangkalian atau kesan daripada insiden akan datang.	
012701 Pengalaman Dari Insiden Keselamatan Maklumat	**Tanggungjawab**
Pengetahuan dan pengalaman yang diperoleh daripada analisis dan penyelesaian insiden keselamatan maklumat hendaklah digunakan untuk mengurangkan kemungkinan insiden berulang serta meminimumkan kesannya pada masa hadapan. Setiap insiden keselamatan maklumat hendaklah direkodkan, dan penilaian menyeluruh perlu dilaksanakan bagi memastikan kawalan yang diambil mencukupi atau perlu dipertingkatkan. Maklumat yang diperoleh daripada penilaian insiden ini hendaklah digunakan untuk: a) **Menambah baik pelan pengurusan insiden**, termasuk penyemakan semula senario dan prosedur berkaitan. b) **Mengenal pasti insiden berulang atau serius serta puncanya** bagi mengemas kini penilaian risiko keselamatan maklumat organisasi. Ini termasuk menentukan dan melaksanakan kawalan tambahan untuk **mengurangkan kemungkinan serta impak insiden serupa di masa hadapan**. Mekanisme yang boleh digunakan termasuk **pengumpulan, pengukuran, dan pemantauan**	ICTSO, BTM dan CERT PKPMP

data berkaitan jenis insiden, kekerapan kejadian, serta kos yang terlibat. c) **Meningkatkan kesedaran dan latihan pengguna** dengan menyediakan contoh insiden sebenar, panduan bertindak balas, serta langkah-langkah pencegahan untuk mengelakkan kejadian yang sama berulang.	

0128 Pengumpulan Bahan Bukti

Objektif:

Memastikan pengurusan bukti yang konsisten dan efektif berkaitan dengan insiden keselamatan maklumat bagi tujuan tindakan disiplin dan undang-undang.

012801 Pengumpulan Bahan Bukti	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti yang berikut: a) Prosedur untuk mengenal pasti, mengumpul, mendapatkan dan menyimpan bahan bukti hendaklah dibangunkan bagi memastikan bahan bukti dilindungi dan tersedia. Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti.	ICTSO, BTM dan CERT PKPMP

0129 Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

Objektif:

Keselamatan maklumat hendaklah diberi penekanan dalam sistem pengurusan kesinambungan organisasi.

012901 Rancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	**Tanggungjawab**
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	CDO dan Pasukan Pemulihan Bencana

mengenal pasti keselamatan maklumat pada lokasi kesinambungan perkhidmatan. Pelan ini mestilah diluluskan oleh CDO.	
012902 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	**Tanggungjawab**
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) Mengenal pasti aspek keselamatan dalam membangunkan pelan kesinambungan keselamatan. b) Mengenal pasti semua aset, tanggungjawab, struktur organisasi dan menetapkan prosedur kecemasan atau pemulihan amalan terbaik. c) Mengenal pasti peristiwa atau ancaman yang boleh mengakibatkan gangguan terhadap proses organisasi. d) Mengenal pasti 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.	CDO dan Pasukan Pemulihan Bencana

i) Membuat pendua (*backup*) mengikut prosedur yang ditetapkan.

j) Menguji, menyelenggara dan mengemaskini Pelan Pemulihan Bencana ICT sekurang-kurangnya setahun sekali.

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 dikenal pasti 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.

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.	
0130 Kesediaan ICT Untuk Kesinambungan Perkhidmatan	
Objektif: Memastikan maklumat dan aset ICT PKPMP tersedia apabila berlaku gangguan.	
013001 Mengkaji, Mengesah Dan Menilai Kesinambungan Perkhidmatan Maklumat	**Tanggungjawab**
PKPMP hendaklah mengkaji, mengesah dan menilai tahap keselamatan maklumat yang diwujudkan dan disimpan di lokasi kesinambungan perkhidmatan. PKPMP hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan sekurang-kurangnya setahun sekali bagi memastikannya terpakai dan berkesan semasa situasi kecemasan.	CDO, Pasukan Pemulihan Bencana dan ICTSO

Kesediaan ICT hendaklah dirancang, dilaksanakan, diselenggara dan diuji berdasarkan objektif kesinambungan perniagaan dan keperluan kesinambungan ICT. PKPMP hendaklah memastikan bahawa:

a) Struktur pasukan PKP yang mencukupi disediakan untuk menyediakan, mengurangkan dan bertindak balas terhadap gangguan.

b) Pelan PKP dan pelan-pelan lain yang terlibat termasuk tindak balas dan prosedur pemulihan hendaklah dinilai dan diuji melalui pelaksanaan simulasi sekurang-kurangnya setahun sekali serta diluluskan oleh pihak pengurusan.

c) Pelan PKP hendaklah mengandungi perkara seperti yang berikut:

   i) spesifikasi prestasi dan kapasiti untuk memenuhi keperluan dan objektif kesinambungan perniagaan seperti yang dinyatakan dalam BIA.

   ii) Objektif Masa Pemulihan (RTO) bagi setiap perkhidmatan ICT mengikut keutamaan pemulihan dan prosedur untuk memulihkan komponen tersebut.

   iii) Objektif Titik Pemulihan (RPO) bagi setiap perkhidmatan ICT mengikut keutamaan pemulihan dan prosedur untuk memulihkan komponen tersebut.

0131 Keperluan Undang-Undang, Peraturan Dan Kontrak	
Objektif: Meningkat dan memantapkan tahap keselamatan siber bagi mengelakkan pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	
013101 Mengenal Pasti Keperluan Undang-Undang Dan Perjanjian Kontrak	**Tanggungjawab**
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga PKPMP dan pembekal serta semua pihak yang terlibat dalam pembekalan perkhidatan ICT di PKPMP. 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
0132 Hak Harta Intelek (*Intellectual Property Rights* - IPR)	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak yang berkaitan dengan hak harta intelek dan pengunaan hak milik produk.	
013201 Hak Harta Intelek (Intellectual Property Rights - IPR)	**Tanggungjawab**
PKPMP akan mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. perkara yang perlu dipatuhi adalah seperti yang berikut	Semua Pengguna

a) Keperluan hak cipta yang berkaitan dengan bahan proprietari, perisian, dan rekabentuk yang diperolehi daripada PKPMP. b) Keperluan perlesenan menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperolehi oleh PKPMP. c) PKPMP perlu memastikan pematuhan berterusan dengan sekatan hak cipta produk dan keperluan perlesenan. d) Pengguna tidak dibenarkan daripada menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan. e) Semua pihak yang terlibat hendaklah melaksanakan kawalan terhadap keperluan perlesenan supaya PKPMP menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	
0133 Perlindungan Rekod	
Objektif: Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak serta jangkaan masyarakat atau sosial berkaitan perlindungan dan ketersediaan rekod.	
013301 Perlindungan Rekod	**Tanggungjawab**
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 adalah seperti yang berikut:	Semua Pengguna

a) Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat. b) Jadual penyimpanan rekod perlu dikenal pasti. c) Inventori rekod.	

0134 Privasi Dan Perlindungan Maklumat Peribadi

Objektif:

Memastikan pematuhan kepada keperluan undang-undang, peraturan dan kontrak berkaitan aspek keselamatan maklumat dalam perlindungan maklumat pengecaman individu.

013401 Privasi dan Perlindungan Maklumat Peribadi	**Tanggungjawab**
Maklumat peribadi merujuk kepada sebarang data yang boleh digunakan untuk mengenal pasti individu seperti nombor kad pengenalan, rekod perubatan dan lain-lain. Jika terdapat sebarang keperluan terhadap pengenalan tersebut hendaklah terlebih dahulu mendapat persetujuan daripada individu berkenaan. Pelaksanaan perlindungan maklumat peribadi di PKPMP selaras dengan peruntukan yang dinyatakan dalam Akta Perlindungan Data Peribadi yang terkini.	Semua Pengguna

0135 Kajian Keselamatan Maklumat

Objektif:

Memastikan kesesuaian, kecekapan dan keberkesanan yang berterusan dalam pendekatan PKPMP untuk menguruskan keselamatan maklumat.

013501 Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat	**Tanggungjawab**
Perlaksanan keselamatan maklumat PKPMP hendaklah dikaji secara bebas atau oleh pihak ketiga pada jangka masa	CDO dan JKP ISMS

yang dirancang atau apabila terdapat perubahan ketara berlaku dalam perlaksanaannya.	
0136 Pematuhan Kepada Dasar, Peraturan Dan Piawaian Keselamatan Maklumat	
Objektif: Memastikan keselamatan maklumat yang dilaksanakan dan beroperasi sesuai dengan polisi keselamatan, polisi tajuk khusus, peraturan dan piawaian yang dikaji semula secara berkala.	
013601 Pematuhan Dasar dan Standard/Piawaian Keselamatan Maklumat	**Tanggungjawab**
PKPMP hendaklah membuat kajian semula pematuhan dan prosedur pemprosesan maklumat dalam kawasan tanggungjawab mereka dengan PKS PKPMP dan piawaian yang berkenaan. Kajian teknikal perlu dilakukan dua (2) tahun sekali. Sekiranya kajian semula mengenal pasti ketidakpatuhan, PKPMP perlu mengambil langkah seperti yang berikut: 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 kekurangan dan kelemahan.	CDO dan JKP ISMS
013602 Kajian Semula Pematuhan Teknikal	**Tanggungjawab**
Sistem maklumat hendaklah dikaji supaya selaras dengan pematuhan dasar dan standard keselamatan maklumat organisasi (Contohnya, Kajian *Security Posture Assessment*	Pentadbir ICT, Pengurus ICT dan ICTSO

– SPA). Kajian teknikal perlu dilakukan dua (2) tahun sekali atau mengikut kesesuaian.	

0137 Dokumentasi Prosedur Operasi Standard

Objektif:

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas kemudahan pemprosesan maklumat.

013701 Dokumentasi Prosedur Operasi Standard	**Tanggungjawab**
Bagi memastikan kemudahan pemprosesan maklumat beroperasi seperti yang telah ditetapkan dan selamat, perkara yang perlu dipatuhi adalah seperti yang berikut: a) Semua prosedur keselamatan siber yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumenkan, 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. Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pengurus ICT, Pentadbir ICT dan ICTSO

2. BIDANG 02 KAWALAN MANUSIA

0201 Tapisan Keselamatan (*Security Screening*)

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.

020101 Tapisan Keselamatan (*Security Screening*)	**Tanggungjawab**
Tapisan keselamatan hendaklah dijalankan terhadap warga PKPMP, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPMP yang terlibat selaras dengan keperluan perkhidmatan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga PKPMP, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPMP yang terlibat dalam menjamin keselamatan aset maklumat sebelum, semasa dan selepas perkhidmatan. b) Menjalankan tapisan keselamatan untuk warga PKPMP, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPMP 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 dan Pengguna Luar

0202 Terma & Dan Syarat Perkhidmatan	
Objektif: Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
020201 Terma & Dan Syarat Perkhidmatan	**Tanggungjawab**
Persetujuan berkontrak dengan Warga PKPMP, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di PKPMP hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga PKPMP, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPMP yang terlibat dalam menjamin keselamatan aset ICT. 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 dan Pengguna Luar
0203 Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat	
Objektif: Memastikan kakitangan dan pihak yang berkepentingan sedar dan memenuhi tanggungjawab keselamatan maklumat.	
020301 Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat	**Tanggungjawab**
Warga PKPMP, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPMP perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai PKS PKPMP, sistem pengurusan keselamatan	ICTSO, Cawangan Pengurusan Sumber

maklumat dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Melaksanakan kesedaran, pendidikan dan latihan berkaitan dengan pengurusan keselamatan ICT kepada pengguna PKPMP dan pengguna luar diberikan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. b) PKPMP perlu menyediakan kesedaran, pendidikan dan latihan 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.	Manusia, Pengurus ICT, Pengguna PKPMP & Pengguna Luar

0204 Proses Tatatertib

Objektif:

Memastikan kakitangan dan pihak yang berkepentingan faham ke atas kesan perlanggaran polisi keselamatan, menghalang dan berurusan dengan kakitangan serta pihak yang berkepentingan yang terlibat dengan perlanggaran.

020401 Proses Tatatertib	**Tanggungjawab**
Proses tatatertib yang formal perlu ditentukan dan disampaikan kepada warga PKPMP atau pihak berkepentingan terlibat yang lain bagi membolehkan tindakan diambil ke atas pelanggaran	ICTSO, Cawangan Pengurusan Sumber

keselamatan maklumat yang dilakukan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan PKPMP serta pengguna luar sekiranya berlaku perlanggaran terhadap polisi, perundangan dan peraturan ditetapkan oleh PKPMP atau Kerajaan. b) Tindakan tatatertib atau Tindakan yang sewajarnya akan dikenakan bagi sebarang pelanggaran kepada polisi ini.	Manusia, Pengurus ICT, Pengguna PKPMP dan Pengguna Luar
0205 Tanggungjawab Selepas Pertukaran Atau Penamatan Peranan Atau Perkhidmatan	
Objektif: Melindungi pihak berkepentingan PKPMP sebagai sebahagian proses pertukaran atau penamatan kakitangan atau kontrak.	
020501 Pertukaran atau Penamatan Peranan Atau Perkhidmatan	**Tanggungjawab**
Peranan dan tanggungjawab berkaitan keselamatan maklumat yang masih sah selepas penamatan atau pertukaran perjawatan hendaklah ditentukan, dikuat kuasa dan disampaikan kepada Warga PKPMP dan semua pihak yang terlibat. Semua Warga PKPMP dan pembekal serta pihak yang terlibat dengan perkhidmatan ICT PKPMP yang telah tamat peranan atau perkhidmatan perlu mematuhi perkara berikut seperti yang berikut: a) Memastikan semua aset maklumat milik PKPMP atau Kerajaan dikembalikan kepada PKPMP mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses	ICTSO, Cawangan Pengurusan Sumber Manusia, Pengurus ICT, Pengguna PKPMP dan Pengguna Luar

maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. c) Maklumat rasmi dalam aset maklumat tidak dibenarkan dibawa keluar dari PKPMP. Warga PKPMP yang bertukar keluar atau tamat perkhidmatan di PKPMP hendaklah: a) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada PKPMP mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. b) Membatalkan atau menarik semula semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan oleh PKPMP. c) Menyediakan dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	

0206 Perjanjian Kerahsiaan (*Non-Disclosure Agreement*) Maklumat	
Objektif: Mengekalkan kerahsiaan maklumat yang boleh dicapai oleh kakitangan dan pihak luaran/ketiga.	
020601 Perjanjian Kerahsiaan (*Non-Disclosure Agreement*) Maklumat	**Tanggungjawab**
Syarat-syarat perjanjian kerahsiaan atau ketakdedahan (*non-disclosure agreement*) perlu mengambil kira keperluan organisasi dan hendaklah dikenal pasti dan dokumentasikan serta ditandatangani oleh warga PKPMP dan pihak berkepentingan terlibat yang lain.	CDO, BTM dan ICTSO

Pembekal atau pihak berkepentingan yang terlibat dengan perkhidmatan ICT PKPMP hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan. Perjanjian kerahsiaan dan ketakdedahan bagi setiap pembekal atau pihak berkepentingan yang terlibat dengan perkhidmatan ICT PKPMP ini perlu disemak secara berkala sekurang-kurangnya sekali dalam tempoh setahun bagi memastikan senarai pihak pembekal atau pihak yang terlibat dengan perkhidmatan ICT PKPMP.	

0207 Bekerja Secara Jarak Jauh (*Remote Working*)	
Objektif: Memastikan Keselamatan kerja jarak jauh dan penggunaan peranti mudah alih.	
020701 Dasar Peranti Mudah Alih dan Bekerja Secara Jarak Jauh	**Tanggungjawab**
Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti yang 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.	ICTSO, Cawangan Pengurusan Sumber Manusia, Pengurus ICT, Pengguna PKPMP & Pengguna Luar

e) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan. Dasar dan langkah-langkah keselamatan hendaklah dilaksanakan bagi melindungi maklumat yang dicapai, diproses atau disimpan secara jarak jauh. Warga PKPMP yang bekerja jarak jauh hendaklah: a) memastikan keselamatan maklumat jabatan dipatuhi dan tidak disebarkan kepada pihak ketiga. b) memastikan arahan bekerja dari luar dipatuhi mengikut garis panduan yang ditetapkan.	
0208 Pelaporan Insiden Keselamatan Maklumat	
Objektif: Menyokong pelaporan bagi kejadian keselamatan maklumat yang boleh dikenalpasti oleh kakitangan tepat pada masanya, konsisten dan berkesan.	
020801 Mekanisme Pelaporan Insiden Keselamatan Maklumat	**Tanggungjawab**
Insiden keselamatan ICT atau ancaman yang mungkin berlaku ke atas aset ICT yang melanggar Polisi Keselamatan Siber (PKS) 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 *Goverment Computer Emergency Response Team* (GCERT) Agensi Keselamatan Negara (NACSA) dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:	CDO

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.
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.
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.	
020802 Melaporkan Kelemahan Keselamatan ICT	**Tanggungjawab**
Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat PKPMP dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.	Semua Pengguna

3. BIDANG 03 KAWALAN FIZIKAL

0301 Perimeter Keselamatan Fizikal

Objektif:

Mencegah akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat PKPMP.

030101 Kawalan Perimeter Keselamatan Fizikal	Tanggungjawab
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Perkara yang perlu dipatuhi adalah seperti yang 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) Mengehadkan 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	Seksyen Keselamatan Bahagian Pengurusan, CDO dan ICTSO

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 daripada kebakaran, banjir, letupan, kacau-bilau dan bencana. k) Menyediakan garis panduan untuk kakitangan yang bekerja dalam kawasan terhad. l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya. m) Rekod log bagi kad akses ke pintu-pintu kawalan mestilah disemak sekurang-kurangnya setahun sekali atau sekiranya terdapat keperluan atau perubahan. n) Pelawat perlu diiringi oleh kakitangan PKPMP yang berkaitan.	
0302 Laluan Keluar Masuk Fizikal	
Objektif: Memastikan penggunaan laluan masuk fizikal kepada maklumat dan aset ICT PKPMP yang disahkan sahaja.	
030201 Kawalan Keluar Masuk Fizikal	**Tanggungjawab**
Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis PKPMP. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Setiap pegawai dan kakitangan PKPMP hendaklah mempamerkan pas keselamatan sepanjang waktu	Pengguna PKPMP, Pengguna Luar dan Seksyen Keselamatan

bertugas. Semua pas keselamatan hendaklah dikembalikan kepada PKPMP apabila pegawai dan kakitangan bertukar tempat bertugas, tamat perkhidmatan atau bersara. b) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan semula selepas tamat lawatan. c) Kehilangan pas keselamatan mestilah dilaporkan dengan segera kepada Seksyen Keselamatan. d) Setiap pelawat hendaklah mendaftar kehadiran dalam buku pelawat di kaunter utama.	Bahagian Pengurusan
030202 Kawasan Penghantaran dan Pemunggahan	**Tanggungjawab**
PKPMP hendaklah memastikan kawasan penghantaran dan pemunggahan serta tempat-tempat lain juga dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	ICTSO, Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK) dan Seksyen Keselamatan Bahagian Pengurusan
0303 Keselamatan Pejabat, Bilik dan Kemudahan	
Objektif: Mencegah dari akses fizikal yang tidak sah, kerosakan dan gangguan terhadap maklumat dan aset ICT PKPMP di pejabat, bilik dan kemudahan.	
030301 Keselamatan Pejabat, Bilik dan Kemudahan	**Tanggungjawab**
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:	ICTSO dan Seksyen Keselamatan

Kawasan tempat bekerja, bilik mesyuarat, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan kamera litar tertutup (CCTV) dan pusat data perlu dihadkan daripada dicapai tanpa kebenaran. a) Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada dicapai oleh orang luar. b) Penunjuk lokasi bilik operasi dan tempat larangan mematuhi arahan keselamatan.	Bahagian Pengurusan

0304 Pemantauan Keselamatan Fizikal

Objektif:

Mengesan dan menghalang akses fizikal yang tidak sah.

030401 Pemantauan Keselamatan Fizikal	**Tanggungjawab**
Premis fizikal harus dipantau oleh sistem pengawasan termasuk pengawal, penggera penceroboh, sistem pemantauan video seperti CCTV dan perisian pengurusan maklumat keselamatan fizikal sama ada diurus secara dalaman atau oleh penyedia perkhidmatan pemantauan. Sistem pemantauan harus dilindungi daripada capaian yang tidak dibenarkan untuk mengelakkan maklumat pengawasan, seperti suapan video, daripada dicapai oleh orang yang tidak dibenarkan atau sistem diceroboh secara jarak jauh. Melaksanakan pemantauan secara berterusan di premis bagi mengelakkan capaian secara fizikal yang tidak dibenarkan. Capaian kepada bangunan yang menempatkan sistem kritikal harus dipantau secara berterusan untuk mengesan	Seksyen Keselamatan Bahagian Pengurusan

capaianyang tidak dibenarkan atau tingkah laku yang mencurigakan dengan: a) Memasang sistem pemantauan video seperti CCTV untuk melihat dan merakam capaian ke kawasan sensitif di dalam dan di luar premis PKPMP b) Memasang, mengikut piawaian terpakai yang berkaitan, dan menguji pengesan sentuhan, bunyi atau gerakan secara berkala untuk mencetuskan penggera pencerobohseperti: i) Memasang pengesan sesentuh yang mencetuskan penggera apabila sesentuh dibuat atau pecah di mana-mana tempat di mana sentuhan boleh dibuat atau dipecahkan (seperti tingkap dan pintu dan di bawah objek) untuk digunakan sebagai penggera panik. ii) Memasang pengesan yang sensitif kepada bunyi kaca pecah yang boleh digunakan untuk mencetuskan penggera bagi memberi amaran kepada kakitangan keselamatan. iii) Menggunakan penggera tersebut untuk melindungi semua pintu luar dan tingkap yang boleh dicapai. Kawasan yang tidak berpenghuni perlu sentiasa diberi perhatian. iv) Perlindungan juga perlu disediakan untuk kawasan lain (contoh: komputer atau bilik komunikasi).	

0305 Perlindungan Terhadap Ancaman Fizikal Dan Persekitaran
Objektif: Mencegah atau mengurangkan kesan dari kejadian yang berpunca dari ancaman fizikal dan persekitaran.

030501 Perlindungan Terhadap Ancaman Fizikal Dan Persekitaran	Tanggungjawab
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. PKPMP perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	ICTSO dan Seksyen Keselamatan Bahagian Pengurusan
0306 Bekerja Di Kawasan Selamat (*Working In Secure Area*)	
Objektif: Mencegah maklumat dan aset ICT di dalam kawasan yang selamat dari kerosakan dan gangguan oleh kakitangan yang tidak sah yang bekerja di kawasan tersebut.	
030601 Bekerja Di Kawasan Selamat (*Working In Secure Area*)	**Tanggungjawab**
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai yang diberi kebenaran sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat dalam kawasan tersebut. Pejabat operasi ICT PKPMP, Bilik *Server* dan Pusat Data (*Data Centre*) berada dalam kawasan larangan. Perkara yang perlu dipatuhi adalah seperti yang 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.	ICTSO dan Seksyen Keselamatan Bahagian Pengurusan

c) Bilik dalam kawasan larangan perlu dikunci pada setiap masa. d) Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk melainkan dengan kebenaran. 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 didaftarkan dalam sistem dan rekod pengecaman muka dan cap jari bagi tujuan akses.	

0307 Polisi *Clear Desk* Dan *Clear Screen*

Objektif:

Mengurangkan risiko capaian tidak sah, kehilangan dan kerosakan kepada maklumat di meja, skrin dan mana-mana lokasi yang boleh dimasuki sewaktu dan selepas waktu bekerja.

030701 Polisi Clear Desk Dan Clear Screen	**Tanggungjawab**
Polisi *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna, pada paparan skrin komputer, mesin pencetak, mesin faksimile atau mesin pengimbas apabila pengguna tidak berada di tempatnya. Polisi *Clear Desk* dan *Clear Screen* ialah satu set garis panduan yang digunakan dalam pengurusan keselamatan maklumat dan	Semua Pengguna

keberkesanan dalam organisasi untuk melindungi maklumat sensitif dan menjaga privasi pekerja. Objektif utama polisi ini adalah untuk memastikan data dan maklumat terjamin keselamatannya dan tidak didedahkan kepada pihak yang tidak mempunyai hak capaian ke atas data atau maklumat tersebut. Polisi ini merangkumi aspek seperti yang berikut:

a) Penggunaan fungsi kata laluan penyelamat skrin (*screen saver password*) atau log keluar apabila meninggalkan komputer.
b) Pengaktifan fungsi mod senyap.
c) Penyimpanan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci.
d) Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimile dan mesin fotostat.
e) Pengawalan e-mel masuk dan keluar.
f) Kawalan penggunaan mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.
g) Penetapanan dan hebahan peraturan serta panduan berkaitan konfigurasi mesej timbul (*pop-up message*) di skrin (contohnya, mematikan pop-up e-mel dan mesej baharu semasa pembentangan, perkongsian skrin atau di kawasan awam).
h) Memadamkan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi.

0308 Penempatan Dan Perlindungan Peralatan ICT

Objektif:

Melindungi peralatan ICT PKPMP daripada kehilangan, kerosakan, kecurian dan disalahgunakan.

030801 Penempatan Dan Perlindungan Peralatan ICT	Tanggungjawab
Peralatan ICT hendaklah dijaga dan dikawal selia dengan baik. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Memeriksa dan memastikan semua peralatan ICT di bawah kawalan pengguna berfungsi dengan sempurna. b) Pengguna 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) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya. f) Pengguna hendaklah 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. h) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang 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.	Pengguna PKPMP, Pengguna Luar dan ICTSO

j) Peralatan rangkaian seperti suis, *hub*, *router* dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci. k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai. l) Peralatan ICT yang hendak dibawa ke luar premis, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan. m) Peralatan ICT yang hilang hendaklah dilaporkan segera kepada Ketua Jabatan, ICTSO dan pihak Polis. n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa. o) Pengguna tidak dibenarkan mengubah kedudukan computer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pegawai Aset. p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Sistem Meja Bantuan PKPMP untuk dibaik pulih. q) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik. r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal tanpa kebenaran Pentadbir Aset. s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT. t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang	

digunakan sepenuhnya bagi urusan rasmi Kerajaan dan PKPMP sahaja. u) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.	
030802 Peralatan Dibawa Keluar Permis	**Tanggungjawab**
Peralatan ICT yang hendak dibawa keluar dari premis PKPMP untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Jabatan atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang bertanggungjawab.	Semua Pengguna, Pegawai Aset dan Ketua Jabatan
0309 Keselamatan Peralatan di Luar Premis	
Objektif: Mencegah maklumat dan aset ICT dalam kawasan yang selamat dari kerosakan dan gangguan oleh pihak luar yang tidak sah yang bekerja di kawasan tersebut.	
030901 Keselamatan Peralatan di Luar Premis	**Tanggungjawab**
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis PKPMP. 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 yang berikut:	Semua Pengguna dan Pegawai Aset

a) Peralatan perlu dilindungi dan dikawal sepanjang masa. b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	

0310 Media Storan

Objektif:

Melindungi media storan daripada sebarang keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan serta gangguan ke atas aktiviti perkhidmatan.

031001 Pengurusan Media Storan Mudah Alih (*Removal* Media)	**Tanggungjawab**
Untuk mengelakkan kerosakan pada aset maklumat dan gangguan kepada aktiviti perkhidmatan, media mudah alih harus dikawal dan dilindungi secara fizikal. Media mudah alih mesti dikendalikan mengikut klasifikasi maklumat. Prosedur pengurusan media mudah alih hendaklah dilaksanakan mengikut skim pengelasan yang diguna pakai oleh PKPMP. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: a) Mengawal akses dan menentukan capaian media kepada pengguna yang dibenarkan sahaja. b) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan. c) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan selamat serta mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat.	CDO, Pegawai ICT dan Pengguna

d) Pelupusan Aset ICT hendaklah dilaksanakan mengikut Pekeliling Pengurusan Aset Alih Kerajaan yang berkuat kuasa. e) Pelupusan maklumat hendaklah mengikut Tatacara Pelupusan Arkib Negara (Akta Arkib Negara 2003 [Akta 629])	
031002 Pelupusan Media Storan	**Tanggungjawab**
Pelupusan media storan yang perlu mendapat kelulusan daripada pihak pengurusan BTM, PKPMP dan mengikut prosedur pelupusan aset ICT yang ditetapkan oleh Kerajaan. Media storan yang mengandungi maklumat terperingkat yang hendak disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikt prosedur yang berkuat kuasa adalah seperti yang berikut: a) Pelupusan media storan perlu mendapat kelulusan dari pihak pengurusan BTM, PKPMP. b) Pelupusan media storan yang telah diluluskan perlu mengikut prosedur Tatacara Pelupusan Arkib Negara (Akta Arkib Negara 2003 [Akta 629])	CDO, Pegawai ICT dan Pengguna
031003 Pemindahan Media Storan Fizikal	**Tanggungjawab**
PKPMP hendaklah memastikan media yang mengandungi maklumat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa proses pemindahan.	CDO, Pegawai ICT dan Pengguna
031004 Bring Your Own Device (BYOD)	**Tanggungjawab**
BYOD merupakan peralatan mudah alih persendirian seperti telefon pintar, tablet dan laptop yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian	Pengguna

PKPMP. BYOD yang mengakses rangkaian (*wired* atau *wireless*) PKPMP untuk akses kepada Internet tertakluk kepada PKS PKPMP.

Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD adalah seperti yang berikut:

a) Mengelak risiko kebocoran maklumat rasmi.
b) Mengelakkan ancaman risiko keselamatan ICT.
c) Memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi PKPMP.
d) Meningkatkan integriti data.

Bagi mengawal dan memantau pelaksanaan BYOD, mekanisme kawalan diwujudkan adalah seperti yang berikut:

a) Mendaftarkan penggunaan BYOD yang digunakan melalui AD.
b) Mengaktifkan fungsi keselamatan BYOD seperti penggunaan kata laluan dan pengecaman muka bagi mencegah akses tanpa kebenaran.

Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.

0311 Utiliti Sokongan

Objektif:

Untuk melindungi pusat pemprosesan maklumat dari segala gangguan atau ancaman yang boleh mengakibatkan kehilangan maklumat atau kerosakan perkakasan.

031101 Peralatan Sokongan ICT	Tanggungjawab
a) Semua peralatan sokongan ICT hendaklah dilindungi daripada kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran. b) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS). c) Peralatan sokongan seperti UPS dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan. d) Semua alat sokongan perlu diselenggara dari semasa ke semasa sekurang-kurangnya enam kali setahun.	Pengguna PKPMP, Pengguna Luar dan ICTSO

0312 Keselamatan Kabel	
Objektif: Mencegah maklumat dan aset ICT daripada hilang, rosak dan dikompromi atau gangguan kepada operasi PKPMP berkaitan dengan punca kuasa dan kabel komunikasi.	
031201 Keselamatan Kabel	**Tanggungjawab**
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah keselamatan yang perlu diambil adalah seperti yang berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan.	Pentadbir Pusat Data

b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan. c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan pemintasan maklumat pada kabel. d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui sesalur kabel bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

0313 Penyelenggaraan Peralatan

Objektif:

Peralatan ICT harus diselenggara dengan betul untuk memastikan AIC maklumat terjaga.

031301 Pengasingan Rangkaian	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (PM, CM) b) Memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (PM, CM) c) Memastikan setiap peralatan yang masih mempunyai tempoh jaminan atau tidak, perlu diselenggara dengan betul. (PM, CM) d) Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; (PM, CM) e) (Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual) (PM) yang ditetapkan atau (atas keperluan) (CM); dan f) Melaporkan sebarang kerosakan kepada Pegawai Aset BTM melalui Sistem Meja Bantuan PKPMP. (CM)	Semua Pengguna, Pegawai Aset dan Pengurus ICT

0314 Pelupusan Yang Selamat Atau Penggunaan Semula Peralatan	
Objektif: Pengesahan harus dilakukan selepas maklumat sensitif dan perisian telah dilupuskan atau *overwrite* untuk tujuan pelupusan atau penggunaan semula peralatan.	
031401 Pelupusan Yang Selamat Atau Penggunaan Semula Peralatan	**Tanggungjawab**
Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (*overwrite*) sebelum dilupuskan atau diguna 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 aset maklumat yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan PKPMP. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat. b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya. c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut.	Semua Pengguna, Pegawai Aset dan Ketua Jabatan

d) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa.

e) Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara seperti yang berikut tanpa kebenaran PKPMP:

i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.

ii) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya.

iii) Menyimpan dan memindahkan perkakasan luaran komputer seperti pembesar suara dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di PKPMP.

iv) Memindah keluar dari PKPMP bagi mana-mana peralatan ICT yang hendak dilupuskan.

v) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab PKPMP.

PKPMP bertanggungjawab memastikan segala maklumat rasmi Kerajaan disalin pada media storan pendua sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan bagi tujuan sandaran maklumat.

Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan.

Merujuk pekeliling yang sedang berkuat kuasa seperti:

i) Pelupusan aset: Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa. ii) Pelupusan dokumen: Arahan Keselamatan dan tatacara Jabatan Arkib Negara. Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem pengurusan aset.	

4. BIDANG 04 KAWALAN TEKNOLOGI

0401 Peralatan Pengguna

Objektif:

Melindungi maklumat daripada risiko yang didapati dari penggunaan peralatan oleh pengguna.

040101 Perkakasan Pengguna Tanpa Kawalan	Tanggungjawab
Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara seperti yang 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

0402 Hak Capaian Isitmewa (*Privileged Access Rights*)

Objektif:

Memastikan pengguna, komponen perisian dan perkhidmatan yang sah sahaja diberikan hak capaian istimewa.

040201 Pengurusan Hak Capaian Isitmewa (*Privileged Access Rights*)	Tanggungjawab
Peruntukan dan penggunaan hak capaian istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberikan kawalan dan penyeliaan yang ketat mengikut keperluan skop tugas yang telah dikenal pasti berdasarkan prosedur yang berkuat kuasa.	Pentadbir ICT, Pengurus ICT dan ICTSO

0403 Sekatan Capaian Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem aplikasi.	
040301 Sekatan Capaian Maklumat	**Tanggungjawab**
Capaian kepada fungsi maklumat dan sistem ICT hendaklah dihadkan mengikut dasar kawalan capaian merangkumi perkara yang berikut: a) Tidak membenarkan pengguna yang tidak berdaftar mencapai maklumat terperingkat. b) Menyediakan mekanisme konfigurasi untuk mengawal capaian kepada maklumat dalam sistem, aplikasi dan perkhidmatan. c) Mengawal data yang boleh dicapai oleh pengguna tertentu. d) Mengawal identiti atau kumpulan identiti yang mempunyai hak capaian seperti membaca, menulis, memadam dan melaksanakan (*execute*). e) Menyediakan kawalan capaian fizikal atau logikal untuk mengasingkan aplikasi sensitif, data aplikasi atau sistem. f) Pentadbir sistem hendaklah melaksanakan semakan dan pemantauan secara berkala sekurang-kurangnya setahun sekali bagi memastikan pengguna yang mencapai sistem adalah sah. Penggunaan proses dan teknik pengurusan capaian yang dinamik (*dynamic acess management*) bagi melindungi	ICTSO, Pengurus ICT dan Pentadbir ICT

maklumat sensitif perlu dilaksanakan sekiranya diperlukan dengan mengambil kira keperluan berikut: a) Perlindungan sepanjang kitar hayat maklumat dengan menetapkan peraturan berdasarkan kes penggunaan. b) Mewujudkan operasi, proses memantau dan melapor serta infrastruktur sokongan teknikal. c) Melindungi data dengan menetapkan keperluan pengesahan, menghadkan capaian, melaksanakan penyulitan, menetapkan kebenaran mencetak, merekod capaian pengguna dan penggunaan maklumat serta memberikan amaran sekiranya terdapat percubaan untuk menyalahgunakan maklumat.	

0404 Kawalan Capaian Kepada Kod Sumber	
Objektif: Memastikan supaya kod sumber dikawal dan dikendalikan dengan baik dan selamat.	
040401 Kawalan Capaian Kepada Kod Sumber Program	**Tanggungjawab**
Pembangunan sistem secara sumber luaran (*outsource*) perlu diselia dan dipantau oleh BTM, PKPMP. (A.8.4 *Access to Source Code*) Capaian kepada kod sumber hendaklah dihadkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Log audit perlu dikekalkan kepada semua capaian kepada kod sumber. b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada prosedur kawalan perubahan.	Pentadbir Sistem dan Pengurus ICT

c) Kod sumber untuk semua sistem aplikasi dan perisian hendaklah menjadi hak milik PKPMP. d) Mengurus capaian kepada kod sumber program dan perpustakaan sumber program (program source libraries) mengikut prosedur yang ditetapkan. e) Menyediakan capaian kepada membaca dan menulis ke dalam kod sumber berdasarkan keperluan dan mempunyai keupayaan untuk mengawal risiko kemungkinan mengubah atau menyalah guna kod sumber mengikut prosedur yang ditetapkan.	
0405 Pengesahan Identiti Yang Selamat (*Secure Authentication*)	
Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas maklumat yang terdapat ~~di~~ dalam sistem dan aplikasi.	
040501 Had Kawalan Capaian Maklumat	**Tanggungjawab**
Capaian kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pentadbir ICT, ICTSO, Pengurus ICT
040502 Prosedur Log Masuk Yang Selamat	**Tanggungjawab**
Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut: a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan PKPMP.	Pentadbir ICT, ICTSO, Pengurus ICT

b) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log maşuk terhadap sistem aplikasi. c) Mengawal capaian ke atas aplikasi sistem mengikut prosedur log masuk yang ditetapkan. d) Mewujudkan teknik pengesahan pelbagai faktor (*Multi-Factor Authentication*, MFA) berdasarkan pengkelasan maklumat yang bersesuaian bagi mengesahkan pengenalan diri pengguna. e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan yang kukuh dan berkualiti. f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
040503 Prosedur Log Masuk	**Tanggungjawab**
Capaian kepada sistem dan aplikasi hendaklah dikawal oleh prosedur log-on mengikut keperluan. PKPMP hendaklah mengenal pasti teknik pengesahan log masuk yang sesuai iaitu: a) Tidak memaparkan pengenalan sistem atau aplikasi selagi proses log masuk tidak berjaya. b) Paparkan suatu notis amaran bahawa komputer hanya boleh diakses oleh pengguna yang sah. c) Tidak memberikan bantuan mesej semasa prosedur log masuk. d) Pengesahan log masuk. e) Perlindungan terhadap *Brute-Force* log masuk. f) Log “aktiviti log masuk” yang berjaya dan tidak berjaya. g) Mengadakan amaran keselamatan jika ada potensi percubaan atau pencerobohan log masuk berjaya dikesan.	Pentadbir ICT, ICTSO, Pengurus ICT

h) Memaparkan maklumat berikut setelah selesai log masuk yang berjaya. i) Tarikh dan masa log masuk sebelumnya. ii) Butir-butir percubaan log masuk yang tidak berjaya. iii) Tidak memaparkan kata laluan. iv) Tidak menghantar kata laluan dalam "clear-text" melalui rangkaian. v) Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu. vi) Menghadkan sesi sambungan sekatan untuk aplikasi yang berisiko tinggi.	
040504 Sistem Pengurusan Kata Laluan	**Tanggungjawab**
Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh PKPMP adalah seperti yang berikut: a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa sahaja dalam apa jua keadaan dan sebab. b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi atau setelah mencapai tempoh masa pertukaran kata laluan yang ditetapkan oleh pentadbir sistem. c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan digit, abjad dan simbol kecuali bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad. d) Fungsi kunci skrin (*lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama.	Pengguna, Pentadbir ICT, ICTSO, Pengurus ICT

e) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan ~~di~~ dalam program. f) Kuat kuasa pertukaran kata laluan semasa yang ditetapkan secara automatik oleh sistem (*default password*) selepas membuat pendaftaran kali pertama atau menetapkan semula kata laluan. g) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna. h) Pengguna digalakkan untuk menukar kata laluan sekurang-kurangnya sepuluh (10) bulan sekali atau selepas tempoh masa yang ditetapkan. i) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga identifikasi pengguna capaian diaktifkan semula. j) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

0406 Pengurusan Kapasiti

Objektif:

Memastikan kapasiti yang diperlukan oleh kemudahan pemprosesan maklumat, sumber manusia, pejabat dan kemudahan lain.

040601 Perancangan Kapasiti	**Tanggungjawab**
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang	Pentadbir Sistem, Pentadbir Emel, Pentadbir Pusat

dikehendaki dicapai. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. a) Kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. b) Mempertimbangkan penggunaan pengkomputeran awan bagi pengurusan kapisit yang berkesan, anjal (*elasticity*) dan boleh skala (*scalability*).	Data dan Pengurus ICT
0407 Perlindungan Daripada Perisian Hasad (*Protection from Malware*)	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	
040701 Perlindungan Daripada Perisian ~~Berbahaya~~ Hasad	**Tanggungjawab**
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan perisian hasad hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara yang perlu dilaksanakan bagi memastikan perlindungan aset maklumat daripada perisian hasad ialah seperti yang berikut:	Semua Pengguna, Pentadbir ICT dan ICTSO

a) Pengguna hendaklah merujuk kepada garis panduan yang disediakan. b) Memasang sistem keselamatan untuk mengesan perisian atau program hasad seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat. c) Memasang dan menggunakan perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang yang sedang berkuat kuasa. d) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya. e) Mengemas kini antivirus 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 program kesedaran mengenai ancaman perisian hasad dan cara mengendalikannya. h) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi perisian berbahaya. i) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan. j) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	

k) Menentukan prosedur dan tanggungjawab untuk menangani perlindungan terhadap perisian hasad pada sistem. l) Mengesahkan ketepatan sumber maklumat yang berkaitan dengan perisian hasad.	

0408 Kawalan Kerentanan Teknikal (*Vulnerability*)

Objektif:

Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.

040801 Kawalan dari Ancaman Kerentanan Teknikal (*Vulnerability*)	**Tanggungjawab**
Maklumat berkaitan kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap kerentanan teknikal perlu dilaksanakan untuk melindungi sistem maklumat, perisian, dan infrastruktur teknikal organisasi daripada ancaman dan serangan yang berkaitan dengan kerentanan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi. b) Mengenal pasti, menilai dan menganalisis tahap risiko kerentanan yang wujud dalam sistem, perisian, dan rangkaian PKPMP.	Pentadbir Sistem

c) Melaksanakan tindakan penambahbaikan untuk mengatasi kerentanan yang telah dikenal pasti, termasuk melaksanakan penambahbaikan keselamatan dan konfigurasi semula. d) Memantau sistem dan perisian secara berterusan untuk mengenal pasti kerentanan yang mungkin muncul dalam masa sebenar. e) Melaksana dan memastikan amalan terbaik dalam keselamatan teknikal dan pengurusan kerentanan.	
040802 Kawalan Pemasangan Perisian	**Tanggungjawab**
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
0409 Pengurusan Konfigurasi	
Objektif: Memastikan peralatan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul dengan aturan keselamatan yang diperlukan dan konfigurasi tidak diubah oleh perubahan yang tidak sah dan tidak betul.	
040901 Kawalan Pengurusan Konfigurasi	**Tanggungjawab**
Pengurusan konfigurasi perlu dilaksanakan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul berserta dengan keperluan keselamatan. Konfigurasi tidak diubah tanpa kebenaran berdasarkan	ICTSO, Pengurus ICT dan Pentadbir ICT

prosedur yang ditetapkan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Melindungi capaian terhadap fail konfigurasi mengikut kawalan yang ditetapkan. b) Merekod dan menyimpan sebarang perubahan konfigurasi dengan selamat. c) Memantau konfigurasi untuk mengesahkan tetapan konfigurasi dan menilai kawalan keselamatan.	

0410 Penghapusan Data Dan Maklumat

Objektif:

Mencegah pendedahan maklumat sensitif yang tidak sewajarnya dan mematuhi undang-undang, peraturan dan keperluan kontrak dalam pemadaman data dan maklumat.

041001 Penghapusan Data Dan Maklumat	**Tanggungjawab**
Terdapat banyak rekod dan dokumen yang perlu disediakan dan diselenggara dalam bentuk kertas. 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). Maklumat terperingkat yang disimpan dalam aset maklumat hendaklah dilupuskan mengikut prosedur yang ditetapkan. Perkara yang perlu dipatuhi adalah seperti yang berikut:	Pegawai ICT dan Pengguna

a) Menentukan kaedah penghapusan maklumat yang sesuai selaras dengan keperluan PKPMP. b) Merekod keputusan sebagai bukti penghapusan maklumat. c) Mendapatkan bukti penghapusan maklumat sekiranya menggunakan perkhidmatan pembekal.	

0411 Penyembunyian Data (*Data Masking*)

Objektif:

Mengehadkan pendedahan data sensitif termasuk maklumat data *Personal Identifiable Information* (PII) dan mematuhi keperluan undang-undang, peraturan dan kontrak.

041101 Penyembunyian Data (*Data Masking*)	**Tanggungjawab**
Penyembunyian data dilaksanakan bagi melindungi data sensitif seperti data Personal Identifiable Information (PII), dan data terperingkat dengan mengambil kira keperluan perkhidmatan dan polisi kawalan capaian serta polisi lain yang berkaitan tertakluk kepada keperluan perundangan dan peraturan yang berkuat kuasa. Pelaksanaan penyamaran data ialah berdasarkan prosedur yang ditetapkan. Penyembunyian data diperlukan bagi melindungi data PII dan data sensitif daripada terdedah atau bocor kepada pihak yang tidak bertanggung jawab yang akan menyebabkan imej PKPMP terjejas. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Mengenal pasti klasifikasi data yang perlu dikongsi dengan pihak ketiga. b) Mengenal pasti teknik yang sesuai selaras dengan sensitiviti data.	CDO

c) Memastikan pengguna hanya dapat mencapai data yang minimum yang dibenarkan sahaja.	

0412 Pencegahan Ketirisan Data (DLP)

Objektif:

Untuk mengesan dan mencegah pendedahan dan pengekstrakan maklumat yang tidak dibenarkan oleh individu atau sistem.

041201 Kawalan Pencegahan Ketirisan Data (DLP)	**Tanggungjawab**
Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data. Data dalam sistem, rangkaian dan peralatan lain perlu dilindungi daripada pendedahan dan pengekstrakan data yang tidak sah oleh individu atau sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Mengenal pasti dan mengkelaskan maklumat untuk dilindungi daripada ketirisan. b) Memantau saluran transaksi dan perkongsian data (contohnya, e-mel, pemindahan fail, perkhidmatan peranti atau media mudah alih). c) Melaksanakan tindakan pengukuhan untuk mengelakkan ketirisan maklumat.	Pentadbir sistem ICT

0413 Sandaran Maklumat (*Information Backup*)

Objektif:

Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.

041301 Sandaran Maklumat (*Information Backup*)	Tanggungjawab
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara berkala mengikut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off site*. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru. b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat. c) Menguji sistem sandaran 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. f) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan dan tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat.	Pengguna PKPMP dan Pentadbir ICT

0414 Lewahan (*Redundancy*) Bagi Kemudahan Pemprosesan Maklumat	
Objektif: Memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.	
041401 Ketersediaan Kemudahan Pemprosesan Maklumat	**Tanggungjawab**
PKPMP perlu mengenal pasti keperluan, mereka bentuk dan melaksanakan lewahan untuk memastikan kesinambungan perkhidmatan dan ketersediaan kemudahan pemprosesan maklumat. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Mengenal pasti keperluan dan tahap kritikal bagi ketersediaan perkhidmatan dan sistem maklumat. b) Menyediakan lewahan bagi kemudahan pemprosesan maklumat yang dikenal pasti. c) Menguji keberkesanan (*failover testing*) untuk memastikan keberkesanan kemudahan lewahan secara berkala. d) Menyediakan mekanisme yang bersesuaian untuk memberi amaran gangguan atau kegagalan kemudahan pemprosesan maklumat kepada pemilik sistem untuk memastikan lewahan tersebut boleh mengambil alih fungsi kemudahan utama dibaiki atau diganti.	ICTSO dan BTM

0415 Log dan Pemantauan
Objektif: Merekod kejadian, menjana pembuktian, memastikan integriti maklumat log, mencegah capaian tidak sah, mengenal pasti kejadian keselamatan maklumat yang membawa kepada insiden keselamatan maklumat dan menyokong penyiasatan.

041501 Jejak Audit	Tanggungjawab
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. 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. iv) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. v) Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat. vi) 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.	Pengguna PKPMP, Pentadbir Sistem, Pentadbir Emel, Pentadbir Rangkaian dan ICTSO

041502 Perlindungan Log	Tanggungjawab
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
041503 Analisis Log pentadbir dan Operator	**Tanggungjawab**
Analisis log perlu merangkumi analisis dan interpretasi aktiviti keselamatan maklumat untuk mengenal pasti aktiviti yang luar biasa atau tingkah laku yang janggal yang menunjukkan indikator sistem terjejas. Perkara yang perlu dipatuhi adalah seperti yang berikut: 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 diwujudkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.	Pentadbir Pusat Data, Pentadbir Sistem, Pentadbir Rangkaian, Pentadbir Emel dan ICTSO

e) Aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CDO.	

0416 Aktiviti Pemantauan

Objektif:

Mengesan tingkah laku anomali dan potensi kepada insiden keselamatan maklumat.

041601 Pemantauan Berterusan	**Tanggungjawab**
Rangkaian, sistem dan aplikasi harus dipantau dan tindakan sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat. Pentadbir Sistem perlu memantau untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat. Pemantauan kepada rangkaian, sistem dan aplikasi perlu dilaksanakan secara berterusan mengikut tempoh yang bersesuaian. Perkara yang memerlukan pemantauan termasuklah tetapi tidak terhad kepada: a) Trafik keluar masuk rangkaian, sistem dan aplikasi. b) Capaian kepada sistem, pelayan dan perkakasan rangkaian yang kritikal dan sebagainya. c) Tahap pentadbir sistem dan fail konfigurasi rangkaian. d) Log daripada peralatan/perisian keselamatan (contoh: antivirus, IDS, sistem pencegahan pencerobohan (IPS), *firewall* dan lain-lain). e) Log kejadian yang berkaitan aktiviti sistem dan rangkaian. f) Penggunaan kod yang disahkan tidak disalah guna. g) Penggunaan sumber (contohnya, CPU, *hard disks*, *memory* dan *bandwidth*).	Pentadbir Pusat Data, Pentadbir Sistem dan Pentadbir Rangkaian

0417 Penyegerakan Jam (*Clock Synchronisation*)	
Objektif: Membolehkan korelasi dan analisis kejadian berkaitan keselamatan dan lain-lain data yang direkodkan dan untuk menyokong siasatan kepada insiden keselamatan maklumat.	
041701 Penyegerakan Jam (Clock Synchronisation)	**Tanggungjawab**
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam PKPMP atau domain keselamatan perlu diselaraskan dengan waktu paiwai Malaysia yang ditetapkan oleh Masa Standard Malaysia sebagai waktu rujukan utama.	Pentadbir Pusat Data
0418 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa	
Objektif: Memastikan penggunaan program utiliti tidak mendatangkan mudarat kepada keselamatan maklumat bagi kawalan sistem dan aplikasi.	
041801 Penggunaan Utiliti Sistem Yang Mempunyai Hak Istimewa	**Tanggungjawab**
Penggunaan program utiliti yang boleh mengatasi (*overriding*) kawalan sistem dan aplikasi hendaklah dikawal dan dihadkan kepada pegawai yang dibenarkan sahaja. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Had penggunaan program utiliti kepada bilangan praktikal minimum pengguna yang dipercayai dan dibenarkan. b) Penggunaan prosedur pengenalan, pengesahan dan kebenaran untuk program utiliti, termasuk pengenalan unik pengguna program utiliti. c) Mentakrifkan dan mendokumentasikan tahap kebenaran untuk program utiliti.	Pentadbir ICT

d) Kebenaran untuk menggunakan program utiliti secara ad hoc. e) Melaksanakan pengasingan tugas dengan menghadkan capaian pengguna yang mempunyai capaian kepada program utiliti. f) Mengalih keluar atau melumpuhkan semua program utiliti yang tidak diperlukan. g) Mengehadkan ketersediaan program utiliti. h) Pengelogan semua penggunaan program utiliti.	

0419 Kawalan Perisian Operasi Pemasangan Perisian Pada Sistem Operasi

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

041901 Kawalan Perisian Operasi	**Tanggungjawab**
Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut: 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.	Pentadbir Sistem dan Pengurus ICT

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) Setiap konfigurasi ke atas sistem perlu dikawal dan didokumentasikan melalui satu sistem kawalan konfigurasi. Konfigurasi hanya boleh dilaksanakan selepas mendapat persetujuan dari pihak berkaitan. h) Satu "*rollback*" strategi harus diadakan sebelum perubahan dilaksanakan.	

0420 Keselamatan Rangkaian	
Objektif: Memastikan perlindungan pemprosesan maklumat dalam rangkaian.	
042001 Kawalan Infrastruktur Rangkaian	**Tanggungjawab**
Infrastruktur rangkaian hendaklah dikawal dan diuruskan sebaik mungkin dalam infrastruktur rangkaian daripada sebarang ancaman demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Perkara yang perlu dipatuhi adalah seperti yang 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.	Pengguna, Pentadbir Rangkaian dan ICTSO

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) Tembok keselamatan (*firewall*) hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian.

f) Semua trafik keluar dan masuk rangkaian hendaklah melaluitTembok keselamatan (*firewall*)l di bawah kawalan BTM, PKPMP.

g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada 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 rangkaian tanpa wayar hendaklah dipantau dan dikawal penggunaannya.

m) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan.

n) Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian 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. s) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan PKPMP. Semua peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai antivirus yang sah.	

0421 Keselamatan Pada Perkhidmatan Rangkaian	
Objektif: Memastikan keselamatan dalam penggunaan perkhidmatan rangkaian.	
042101 Keselamatan Perkhidmatan Rangkaian	**Tanggungjawab**
Pegurusan bagi semua perkhidmatan rangkaian dalaman (*inhouse*) dan sumber luar (*outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan	Pentadbir Rangkaian, Pengurus ICT dan ICTSO

rangkaian. Perkara yang mesti dipatuhi adalah seperti yang 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 dalam perjanjian. d) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Agreement* (SLA) yang telah dipersetujui. e) Mempunyai mekanisme pengurusan insiden sekiranya berlaku insiden keselamatan maklumat.	

0422 Pengasingan Rangkaian

Objektif:

Memisahkan rangkaian dalam sempadan keselamatan dan mengawal trafik di kalangan rangkaian tersebut berdasarkan keperluan perkhidmatan PKPMP.

042201 Pengasingan Rangkaian	**Tanggungjawab**
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian PKPMP.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO

0423 Penapisan Web (*Web Filtering*)	
Objektif: Untuk melindungi sistem daripada terjejas oleh perisian hasad dan menghalang akses kepada sumber web yang tidak dibenarkan.	
042301 Kawalan Penapisan Web	**Tanggungjawab**
Kawalan penapisan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat ke laman web yang dianggap tidak selamat dan tidak sesuai supaya dapat melindungi sistem maklumat daripada sebarang ancaman keselamatan laman web luaran. PKPMP hendaklah mengurangkan risiko mencapai laman web yang mengandungi maklumat yang dilarang atau diketahui mengandungi virus atau data pancingan (*phishing*) data oleh pengguna. PKPMP hendaklah mengenal pasti jenis laman web yang patut atau tidak boleh dicapai oleh warga PKPMP. PKPMP hendaklah mempertimbangkan untuk menyekat capaian kepada jenis laman web yang berikut: a) Laman web yang mempunyai fungsi muat naik maklumat melainkan dibenarkan atas sebab perkhidmatan yang sah. b) Tapak web yang diketahui atau disyaki berniat jahat. c) Pelayan arahan dan kawalan (*command and control*). d) Laman web berniat jahat yang diperoleh daripada risikan ancaman. e) Laman web yang berkongsi kandungan haram.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
0424 Penggunaan Kriptografi	

	PKPMP-BTM-ISMS-P1-001 **POLISI KESELAMATAN SIBER PKPMP**

Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
042401 Polisi Penggunaan Kawalan kriptografi	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti yang 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.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
042402 Peraturan Kawalan Kriptografi	**Tanggungjawab**
Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan-peraturan. Perkara yang perlu dipatuhi adalah seperti yang 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.	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
042403 Pengurusan Kunci Kriptografi (*Key Management*)	**Tanggungjawab**
Memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi diguna pakai di PKPMP bagi melindungi kunci berkenaan dari diubah,	Pentadbir Rangkaian,

dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. Setiap urusan transaksi maklumat sensitif secara elektronik hendaklah menggunakan tandatangan digital supaya mendapat perlindungan dan pengiktirafan undang-undang.	Pengurus ICT dan ICTSO
0425 Keselamatan Kitar Hayat Pembangunan Sistem Yang Selamat (SDLC)	
Objektif: Memastikan keselamatan maklumat adalah merupakan sebahagian daripada proses pembangunan sistem. Ini merangkumi keperluan keselamatan maklumat apabila menggunakan rangkaian luar.	
042501 Dasar Pembangunan Sistem Yang Selamat	**Tanggungjawab**
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan untuk perkembangan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang 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 mengenal pasti kelemahan dan mencadangkan penambahbaikan dalam pembangunan sistem.	Pentadbir Sistem dan ICTSO
042502 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat	**Tanggungjawab**

Keperluan keselamatan maklumat bagi pembangunan sistem baharu 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 PKS PKPMP. b) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan. c) Ujian keselamatan hendaklah dilakukan di setiap peringkat pembangunan sistem bagi memastikan kesahihan dan integriti data.	Pemilik Sistem dan Pentadbir Sistem
042503 Kitar Hayat Pembangunan Sistem Yang Selamat	**Tanggungjawab**
Pembangun Sistem hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk Pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. Pembangun Sistem perlu melaksanakan penilaian risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem. b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran. c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem. d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem.	Pembangun Sistem dan Pentadbir Sistem

e) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai. f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	

0426 Keperluan Keselamatan Aplikasi	
Objektif: Memastikan sebarang aplikasi yang dibangunkan atau diperolehi adalah selamat.	
042601 Keperluan Keselamatan Aplikasi	**Tanggungjawab**
Keperluan keselamatan maklumat hendaklah dikenal pasti, ditentukan dan diluluskan sebelum membangunkan atau memperoleh sebarang sistem aplikasi.	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem
042602 Melindungi Perkhidmatan Aplikasi di Rangkaian Umum	**Tanggungjawab**
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 yang berikut: a) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan identiti (*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 aplikasi dan perkhidmatan ICT.	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem

d) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran dan penerimaan dokumen serta kontrak. e) Liabiliti yang berkaitan dengan mana-mana kes transaksi *fraud*. f) Keperluan insuran.	
042603 Melindungi Transaksi Perkhidmatan Aplikasi	**Tanggungjawab**
Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: 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. vi) Pihak yang mengeluarkan dan mengekalkan pensijilan digital atau tandatangan adalah dilantik oleh Kerajaan.	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem

042604 Keperluan Keselamatan Aplikasi	**Tanggungjawab**
Spesifikasi reka bentuk perlu mengandungi keperluan keselamatan sistem maklumat. Sekiranya sesuatu produk perisian aplikasi tersedia (*off-the-shelf*) diperoleh, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.	Pentadbir Sistem dan Pemilik Sistem
0427 Prinsip Keselamatan Arkitektur Dan Kejuruteraan Sistem Yang Selamat (*Secure System Engineering Principles*)	
Objektif: Memastikan aktiviti pembangunan sistem maklumat adalah selamat.	
042701 Prinsip Keselamatan Arkitektur Dan Kejuruteraan Sistem Yang Selamat (*Secure System Engineering Principles*)	**Tanggungjawab**
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini. Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Proses pengemaskinian perisian atau sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan.	Pentadbir Sistem dan Pengurus ICT

b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan. c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan. d) Mengawal capaian ke atas kod atau cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. e) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal. f) Semua sistem konfigurasi perlu didaftar dan didokumenkan.	

0428 Pengaturcaraan Kawalan Kod Selamat

Objektif:

Memastikan perisian ditulis dengan selamat dengan mengurangkan potensi kerentanan (*vulnerability*) keselamatan maklumat dalam perisian.

042801 Pengaturcaraan Kawalan Kod Selamat	**Tanggungjawab**
Persekitaran pembangunan yang selamat hendaklah dibina di atas infrastruktur IT yang boleh dipercayai dan selamat menggunakan 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. e) Log dan Pengauditan.	Pentadbir Sistem ICT PKPMP

0429 Pengujian Dan Penerimaan Keselamatan 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.	
042901 Pengujian Keselamatan Sistem	**Tanggungjawab**
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Semua sistem baharu dan penambahbaikan sistem hendaklah menjalani ujian *Security Posture Assessment* (SPA) termasuk penyediaan jadual terperinci aktiviti, ujian input dan output (*input and output validation*). b) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat. c) Mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi. d) Membuat semakan pengesahan ~~di~~ dalam aplikasi untuk mengenal pasti sebarang pencemaran maklumat sama ada ~~kerana~~ kesilapan atau disengajakan. e) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan. f) Melakukan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem.	Pentadbir Sistem dan ICTSO

g) Menjalankan ujian penembusan untuk mengenal pasti kod dan reka bentuk yang tidak selamat. h) Melaksanakan pengujian keselamatan sistem berdasarkan ISO/IEC/IEEE 29119 *Software Testing Standard* dan garis panduan pengujian keselamatan serta sistem yang sedang berkuat kuasa.	
042902 Pengujian Penerimaan Sistem	**Tanggungjawab**
Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Pengujian penerimaan sistem hendaklah merangkumi keperluan keselamatan sistem maklumat dan kepatuhan kepada polisi pembangunan selamat. b) Penerimaan pengujian semua sistem ~~baru~~ baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai. c) Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian kerentanan (*vulnerability assessment*).	Pentadbir Sistem dan ICTSO
0430 Pembangunan Sistem oleh Pembekal	
Objektif: Memastikan langkah-langkah keselamatan maklumat yang diperlukan oleh PKPMP dilaksanakan oleh pembangun sistem dari pembekal.	
043001 Pembangunan Sistem oleh Pembekal	**Tanggungjawab**
PKPMP hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan menggunakan sumber luar seperti pembekal. Kod sumber yang dibangunkan ialah	Pentadbir Sistem dan Pengurus ICT

HAK MILIK KERAJAAN. Perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Perjanjian lesen, kod sumber ialah **HAK MILIK KERAJAAN** dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi menggunakan sumber luar.

b) Bagi semua perkhidmatan yang disediakan oleh sumber luar, *Software as a Service* (SaaS) yang mengendalikan maklumat rahsia rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko.

c) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik.

d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem.

e) Mengguna pakai prinsip dan tatacara escrow.

f) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.

g) Penyediaan model ancaman (*threat modelling*) untuk dipertimbangkan oleh pembangun sistem serta memastikan tahap keselamatan minimum yang boleh diterima.

h) Peruntukan bukti bahawa ujian yang mencukupi telah digunakan untuk mengawal kehadiran kandungan berniat jahat semasa penghantaran.

i) Peruntukan bukti bahawa ujian yang mencukupi telah digunakan untuk melindungi daripada kelemahan yang diketahui. j) Keperluan keselamatan untuk persekitaran pembangunan. k) Mempertimbangkan perundangan yang berlaku.	

0431 Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi

Objektif:

Melindungi persekitaran produksi dan data dari dikompromi dari aktiviti pembangunan dan pengujian.

043101 Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi	**Tanggungjawab**
a) Persekitaran pembangunan, pengujian dan produksi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara yang perlu dipatuhi adalah seperti yang berikut: b) Perkakasan dan perisian yang digunakan bagi tugas mentakrifkan, mendokumentasikan, membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan daripada perkakasan yang digunakan sebagai produksi. c) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. d) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat. e) Menguji perubahan yang dilaksanakan dalam persekitaran ujian atau persekitaran sementara.	Pentadbir Sistem dan Pengurus ICT

f) Tidak menguji dalam persekitaran produksi kecuali dalam keadaan yang telah ditentukan dan diluluskan. g) Pengkompil, editor dan alat pembangunan atau program utiliti lain yang tidak boleh dicapai daripada sistem pengeluaran apabila tidak diperlukan. h) Memaparkan label yang bersesuaian dengan persekitaran pada menu untuk mengurangkan risiko ralat.	
043102 Persekitaran Pembangunan Selamat	**Tanggungjawab**
Pentadbir Sistem dan Pembangun Sistem hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. PKPMP perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem. b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran. c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem. d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem. e) Pegawai yang bekerja dalam persekitaran pembangunan sistem berintegriti. f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	Pentadbir Sistem dan Pembangun Sistem

0432 Pengurusan Perubahan	
Objektif: Memelihara keselamatan maklumat ketika melaksanakan perubahan.	
043201 Pengurusan Perubahan	**Tanggungjawab**
Tanggungjawab dan tugas perlulah diasingkan untuk mengelakkan perubahan yang tidak dibenarkan atau penyalahgunaan aset PKPMP. Perubahan dalam PKPMP, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti yang 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. d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja ataupun tidak sengaja.	Semua Pengguna, Pengurus ICT dan Pentadbir ICT

043202 Prosedur Kawalan Perubahan Sistem	Tanggungjawab
Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti yang 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. c) Setiap permohonan perubahan/penambahbaikan sistem hendaklah menggunakan Borang Permohonan Perubahan (*Change Request*) untuk memantau perubahan/ penambahbaikan yang dilaksanakan oleh pengaturcara. d) Kawalan perlu dibuat ke atas sebarang perubahan atau pindaan ke atas sistem bagi memastikan ianya terhad mengikut keperluan sahaja. e) Capaian kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	*Change Control Board* dan Pentadbir Sistem
043203 Kajian Semula Keperluan Teknikal Bagi Aplikasi Selepas Perubahan Platform Pengoperasian	**Tanggungjawab**
Perubahan platform pengoperasian hendaklah dikaji semula dan diuji bagi memastikan tiada sebarang masalah yang timbul terhadap operasi atau keselamatan aplikasi. Perkara yang perlu dipatuhi adalah seperti yang berikut:	Pentadbir Sistem dan Pengurus ICT

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.	
043204 Sekatan Perubahan Dalam Pakej Perisian (*Software Packages*)	**Tanggungjawab**
Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan dan terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem, Pengurus ICT dan ICTSO
0433 Maklumat Aktiviti Pengujian	
Objektif: Memastikan perkaitan pengujian dan perlindungan data yang digunakan untuk pengujian.	
043301 Perlindungan Data Ujian	**Tanggungjawab**
Untuk memastikan perlindungan ke atas maklumat yang digunakan untuk pengujian, data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian. b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian.	Pemilik Sistem dan Pentadbir Sistem

c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai. d) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar. e) Melindungi maklumat sensitif melalui penyingkiran atau pengaburan data jika digunakan untuk ujian. f) Memadam maklumat operasi daripada persekitaran ujian serta-merta dengan betul selepas ujian selesai untuk mengelakkan penggunaan maklumat ujian tanpa kebenaran.	

0434 Perlindungan Keselamatan Maklumat Semasa Pelaksanaan Audit	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
043401 Pematuhan Keperluan Audit/Kawalan Audit Sistem Maklumat	**Tanggungjawab**
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. Keperluan dan aktiviti audit yang melibatkan verifikasi sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas fungsi penyampaian perkhidmatan PKPMP. Perkara berikut harus dipatuhi:	ICTSO dan Audit Dalaman

a) Bersetuju dengan permintaan audit untuk mencapai kepada sistem dan data dengan pengurusan yang sesuai. b) Bersetuju dan mengawal skop ujian audit teknikal. c) Mengehadkan ujian audit kepada capaian baca sahaja kepada perisian dan data. Jika capaian baca sahaja tidak tersedia untuk mendapatkan maklumat yang diperlukan, melaksanakan ujian oleh pentadbir berpengalaman yang mempunyai hak capaian yang diperlukan bagi pihak juruaudit. d) Jika capaian diberikan, mewujudkan dan mengesahkan keperluan keselamatan peranti yang digunakan untuk mengcapaian sistem sebelum membenarkan capaian. e) Hanya membenarkan capaian selain daripada baca sahaja untuk salinan terpencil fail sistem, memadamkannya apabila audit selesai, atau memberi mereka perlindungan yang sewajarnya jika terdapat kewajiban untuk menyimpan fail tersebut dibawah keperluan dokumentasi audit. f) Mengenal pasti dan bersetuju dengan permintaan untuk pemprosesan khas atau tambahan, seperti menjalankan alat audit. g) Menjalankan ujian audit yang boleh menjejaskan ketersediaan sistem di luar waktu perniagaan. h) Memantau dan mengelog semua capaian untuk tujuan audit dan ujian.	

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

GLOSARI

	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* 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.

GLOSARI

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.
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.

GLOSARI

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** **POLISI KESELAMATAN SIBER PKPMP**

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER PKPMP

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

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya berjanji bahawa saya akan mematuhi peruntukan Polisi Keselamatan Siber 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 Polisi Keselamatan Siber Jabatan; dan

3. Jika saya ingkar kepada peruntukan–peruntukan yang ditetapkan dan disabitkan kerana melanggar Polisi Keselamatan Siber 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** **POLISI KESELAMATAN SIBER PKPMP** **(PEMBEKAL)**

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER PKPMP (PEMBEKAL)

Nama :……
Jawatan :……
Syarikat :……

Adalah saya _____, nombor kad pengenalan _____ yang mewakili Syarikat _____, No Pendaftaran _____ dengan ini mengaku bahawa perhatian saya telah ditarik kepada Polisi Keselamatan Siber 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 Polisi Keselamatan Siber; 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 POLISI KESELAMATAN SIBER 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;
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;*
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;

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

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.
66. Akta Keselamatan Siber 2024