POLISI KESELAMATAN SIBER

KEMENTERIAN PEMBANGUNAN WANITA, KELUARGA DAN MASYARAKAT

VERSI 2.0

ISI KANDUNGAN

Isi Kandungan

REKOD PINDAAN

VERSI	KELULUSAN	TARIKH KUATKUASA
1.0	JPICT	23 DISEMBER 2022
2.0	JPICT	16 DISEMBER 2025

PENGENALAN

Polisi Keselamatan Siber (PKS) Versi 2.0 ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) di KPWKM dan Agensi. Polisi ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT. Polisi ini adalah terpakai kepada semua kakitangan KPWKM, Agensi dan pihak ketiga yang berurusan dengan KPWKM dan Agensi tersebut.

PKS Versi 2.0 ini berkuat kuasa pada 16 Disember 2025 menggantikan PKS Versi 1.0 yang telah berkuat kuasa pada 23 Disember 2022 hingga 15 Disember 2025.

Agensi di bawah KPWKM adalah seperti berikut:

(a) **JKM** - Jabatan Kebajikan Masyarakat;
(b) **JPW** - Jabatan Pembangunan Wanita;
(c) **LPPKN** - Lembaga Penduduk dan Pembangunan Keluarga Negara;
(d) **ISM** - Institut Sosial Malaysia; dan
(e) **TAGS** -Tribunal bagi Antigangguan Seksual.

OBJEKTIF

Polisi Keselamatan Siber diwujudkan untuk menjamin kesinambungan urusan KPWKM dan Agensi dengan meminimumkan kesan insiden keselamatan siber.

Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi KPWKM dan Agensi. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT adalah seperti berikut:

(a) Memastikan kelancaran operasi KPWKM dan Agensi dan meminimumkan kerosakan atau kemusnahan;
(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan daripada segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

(c) Mencegah salah guna atau kecurian aset ICT Kerajaan;

(d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan; dan

(e) Memperkemaskan pengurusan keselamatan ICT KPWKM.

PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan dimana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan daripada 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-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

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

(a) **Kerahsiaan** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
(b) **Integriti** - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
(c) **Tidak Boleh Disangkal** - Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal;
(d) **Kesahihan** - Data dan maklumat hendaklah dijamin kesahihannya; dan
(e) **Ketersediaan** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain daripada itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Aset ICT KPWKM dan Agensi terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat, manusia dan premis komputer dan komunikasi. Polisi Keselamatan Siber menetapkan keperluan-keperluan asas berikut:

(a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

(b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Polisi Keselamatan Siber ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pengwujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara- perkara berikut:

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KPWKM dan Agensi. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

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

(c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif KPWKM dan Agensi. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod KPWKM dan Agensi, profil-profil.

(e) Manusia

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

(f) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara **(a)** - **(e)** di atas.

(g) Jabatan

Kementerian dan Agensi di bawah KPWKM.

Setiap perkara di atas hendaklah diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan dan hendaklah dipatuhi adalah seperti berikut:

(a) Akses atas dasar perlu mengetahui

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

(b) Hak akses minimum

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

(c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini hendaklah dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu 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 maklumat dan menentukan ianya 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 rahsia rasmi terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

(d) Pengasingan

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat rahsia rasmi atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

(e) Pengauditan

Pengauditan ialah tindakan untuk mengenal pasti insiden keselamatan siber berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta;

Pengauditan juga hendaklah dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer.

Secara keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti. Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:

i. Mengesan pematuhan atau pelanggaran keselamatan;
ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran keselamatan; dan
iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran keselamatan.

(e) Pemulihan

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

(f) Saling Bergantung

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

(g) Pematuhan

Polisi Keselamatan Siber hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

PENILAIAN RISIKO KESELAMATAN ICT

KPWKM dan Agensi hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat daripada ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu, Kementerian hendaklah mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dapat dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

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

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

KPWKM dan Agensi bertanggungjawab melaksanakan dan mengurus risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

KPWKM dan Agensi hendaklah mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
(b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
(c) Mengelak dan/atau mencegah risiko daripada terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
(d) Memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

BIDANG 01: POLISI KESELAMATAN MAKLUMAT

0101 Polisi Keselamatan Maklumat		
Objektif		
Menyediakan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan KPWKM dan Agensi serta tertakluk kepada perundangan yang berkaitan.		
010101 Pengwujudan dan Pelaksanaan Polisi		**Peranan**
	Pengwujudan dan pelaksanaan polisi ini akan dijalankan dengan arahan Ketua Setiausaha (KSU) KPWKM di bantu oleh Pasukan Keselamatan ICT yang terdiri daripada Ketua Pegawai Digital (CDO), SUB/Pengarah, Pegawai Keselamatan ICT (ICTSO) di Kementerian dan Agensi serta pegawai yang dilantik.	KSU KPWKM / Ketua Pegawai Digital (CDO), SUB/ Pengarah, Pegawai Keselamatan ICT (ICTSO) Kementerian dan Agensi
010102 Penyebaran Polisi		**Peranan**
	Polisi ini hendaklah disebarkan kepada semua warga KPWKM (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO KPWKM dan Agensi

BIDANG 01: POLISI KESELAMATAN MAKLUMAT

010103 Penyelenggaraan Polisi		**Peranan**
	Polisi Keselamatan Siber ini hendaklah disemak dan dipinda dari semasa ke semasa mengikut keperluan termasuk kawalan keselamatan, prosedur dan proses selaras dengan kesesuaian, ketepatan dan keberkesanan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur-prosedur yang berhubung dengan penyelenggaraan Polisi Keselamatan Siber: (a) Kajian semula polisi ini hendaklah dibuat semula sekurang - kurangnya dua (2) tahun sekali atau mengikut keperluan semasa; (b) Mengenalpasti dan menentukan perubahan yang diperlukan; dan Cadangan pindaan secara bertulis kepada ICTSO KPWKM dan Agensi untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KPWKM dan memaklumkan kepada semua pengguna perubahan yang telah dipersetujui.	ICTSO KPWKM Dan Agensi
	010104 Pengecualian Polisi	**Peranan**
	Polisi Keselamatan Siber adalah terpakai kepada semua pengguna di Kementerian dan Agensi dan tiada pengecualian diberikan.	Semua Pengguna

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

0201 Infrastruktur Organisasi Dalaman		
Objektif		
Mewujudkan kerangka pengurusan untuk memulakan dan mengawal operasi serta pelaksanaan keselamatan maklumat dalam KPWKM dan Agensi.		
020101 Struktur Tadbir Urus Keselamatan ICT KPWKM		**Peranan**
	Struktur Tadbir Urus Pengurusan Keselamatan ICT adalah seperti carta dibawah:  	JPICT
020102 Jawatankuasa Pemandu ICT		**Peranan**
	Bidang kuasa dan peranan Jawatankuasa Pemandu ICT adalah seperti berikut: (a) Memperakukan/meluluskan dokumen Polisi Keselamatan Siber; dan (b) Memastikan Polisi Keselamatan Siber selaras dengan dasar- dasar Pendigitalan Kerajaan semasa.	JPICT

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

020103 Jawatankuasa Keselamatan ICT KPWKM		**Peranan**
	Bidang kuasa dan peranan Jawatankuasa Keselamatan ICT KPWKM adalah seperti berikut: (a) Polisi Keselamatan Siber selaras dengan dasar-dasar Pendigitalan Kerajaan semasa; (b) Pemantauan tahap pematuhan keselamatan ICT; (c) Penerimaan laporan dan membincangkan hal-hal keselamatan ICT semasa; (d) Membincang tindakan yang melibatkan pelanggaran Polisi Keselamatan Siber; dan (e) Membuat keputusan mengenai tindakan yang mesti diambil mengenai sebarang insiden keselamatan siber.	JKICT
020104 Agensi di bawah KPWKM		**Peranan**
	Bidang kuasa dan peranan agensi di bawah KPWKM adalah seperti berikut: (a) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam KPWKM dan Agensi yang mematuhi keperluan Polisi Keselamatan Siber; dan (b) Melaksana penilaian teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT.	Ketua Bahagian/ Unit IT/Pegawai yang diberi kuasa

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

020105 Ketua Setiausaha KPWKM / Ketua Pengarah Agensi		**Peranan**
	Ketua Setiausaha KPWKM dan Ketua Pengarah Agensi adalah berperanan dan bertanggungjawab dalam perkara- perkara seperti berikut: (a) Semua pengguna hendaklah memahami peruntukan-peruntukan di bawah Polisi Keselamatan Siber; (b) Semua pengguna hendaklah mematuhi Polisi Keselamatan Siber; (c) Semua keperluan KPWKM dan Agensi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; (d) Penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan dalam Polisi Keselamatan Siber; dan (e) Ketua Setiausaha Kementerian atau pegawai yang diturunkan kuasa mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), manakala bagi agensi dipengerusikan oleh Ketua Pengarah Agensi masing-masing.	Ketua Setiausaha KPWKM Ketua Pengarah Agensi
020106 Ketua Pegawai Digital		**Peranan**
	Ketua Pegawai Digital (CDO) adalah seperti berikut: (a) KPWKM – Timbalan Ketua Setiausaha (Pengurusan) KPWKM; (b) JKM – Timbalan Ketua Pengarah (Strategik); (c) JPW – Timbalan Ketua Pengarah; (d) LPPKN – Timbalan Ketua Pengarah (Pengurusan); dan (e) ISM – Timbalan Pengarah.	CDO

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

	Peranan dan tanggungjawab CDO adalah seperti berikut: (a) Membantu Ketua Setiausaha KPWKM dan Ketua Jabatan Agensi dalam melaksanakan tugas- tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan keselamatan ICT; (c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan Polisi Keselamatan Siber serta pengurusan risiko dan pengauditan; dan (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT.	
020107 Pegawai Keselamatan ICT (ICTSO)		**Peranan**
	Pegawai Keselamatan ICT (ICTSO) bagi KPWKM ialah Setiausaha, Bahagian Pengurusan Maklumat (BPM), KPWKM manakala ICTSO bagi Agensi di bawahnya ialah Pegawai Teknologi Maklumat yang dilantik. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Pengurusan keseluruhan program-program keselamatan ICT; (b) Penguatkuasaan pelaksanaan Polisi Keselamatan Siber; (c) Penerangan dan pendedahan berkenaan Polisi Keselamatan Siber kepada semua kakitangan; dan (d) Penyediaan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber; (e) Pelaksanaan pengurusan risiko; (f) Pelaksanaan audit, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (g) Pemakluman amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah	ICTSO

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

	perlindungan yang bersesuaian; (h) Pelaporan insiden keselamatan siber kepada CDO, Pasukan Tindak Balas Insiden Keselamatan siber KPWKM dan Agensi (CSIRT) dan Agensi Keselamatan Siber Negara (NACSA); (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; (j) Penyediaan dan pelaksanaan program-program kesedaran mengenai keselamatan ICT; dan (k) Pelaksanaan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden keselamatan siber baru dapat dielakkan.	
020108 Pengurus ICT		**Peranan**
	Pengurus ICT adalah seperti berikut: (a) KPWKM – Setiausaha Bahagian Pengurusan Maklumat; (b) JKM – Pengarah Bahagian Pengurusan Maklumat; (c) JPW – Pengarah Bahagian Khidmat Pengurusan; (d) LPPKN – Pengarah Bahagian Teknologi Maklumat; dan (e) ISM – Ketua Unit Teknologi Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Polisi Keselamatan Siber hendaklah dibaca, difahami dan dipatuhi; (b) Kajian semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KPWKM dan Agensi; (c) Kawalan akses pengguna terhadap aset ICT KPWKM	Pengurus ICT

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

	dan Agensi ditentukan oleh Pengurus ICT; (d) Pelaporan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; (e) Penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KPWKM dan Agensi; (f) Penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden keselamatan siber baru dapat dielakkan; dan (g) Koordinator kepada Pelan Pemulihan Bencana (DRP).	
020109 Pentadbir Sistem ICT		**Peranan**
	Pentadbir Sistem ICT ialah Pegawai ICT yang dilantik. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Polisi Keselamatan Siber hendaklah dibaca, difahami dan dipatuhi; (b) Kerahsiaan kata laluan hendaklah dijaga; (c) Konfigurasi aset ICT; (d) Tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (e) Tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek; (f) Penentuan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber; (g) Pemantauan aktiviti capaian harian sistem aplikasi pengguna;	Pentadbir Sistem ICT

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

	(h) Pengenalpastian aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (i) Penganalisaan dan penyimpanan rekod jejak audit secara berterusan mengikut piawaian; (j) Penyediaan laporan mengenai aktiviti capaian secara berkala; (k) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya dalam keadaan yang baik; (l) Memastikan pembangunan sistem aplikasi mengambil kira dan mematuhi ciri-ciri keselamatan yang termaktub di dalam Polisi Keselamatan Siber KPWKM; dan (m) Bertanggungjawab memastikan setiap perolehan perisian ICT adalah tulen.	
020110 Pemilik Sistem		**Peranan**
	Sesuatu sistem hendaklah dimiliki oleh sesuatu Unit/Bahagian di KPWKM dan agensi yang mempunyai kepentingan terhadap sistem yang dibangunkan/diurus/digunakan. Pemilik Sistem adalah terdiri daripada Ketua Setiausaha KPWKM dan Ketua Pengarah Agensi atau Ketua Unit/Bahagian yang terlibat dengan sistem yang dibangunkan. Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut: (a) Pelaksanaan promosi sistem kepada pengguna sasaran; (b) Penentuan pengguna dan kategori atau tahap capaian pengguna sistem; (c) Pengurusan senarai pengguna yang terlibat di dalam Latihan Pengguna; (d) Penguatkuasaan penggunaan sistem di kalangan	Pemilik Sistem ICT

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

	pengguna; (e) Pemantauan pelaksanaan dan keberkesanan sistem secara berterusan; (f) Pemakluman sebarang masalah dan keperluan peningkatan sistem kepada Pembangun Sistem; (g) Menentusahkan maklumat rahsia rasmi berdasarkan kandungan taksiran analisis risiko dalam persekitaran pembangunan sistem; (h) Menentusahkan maklumat rahsia rasmi berdasarkan kandungan taksiran analisis risiko dalam persekitaran pembangunan sistem; dan (i) Pemilik Sistem hendaklah melantik seorang pegawai sebagai Pentadbir Sistem untuk tujuan penyelenggaraan sistem tersebut.	
020111 Pentadbir Rangkaian ICT		**Peranan**
	Pentadbir Rangkaian ICT ialah Pegawai ICT yang dilantik. Peranan dan tanggungjawab Pentadbir Rangkaian ICT adalah seperti berikut: (a) Mentadbir akaun pengguna; (b) Merangka, melaksana dan menguatkuasa polisi keselamatan seperti perlindungan dan perkongsian data; (c) Merancang dan melaksana polisi ancaman keselamatan, memantau keadaan rangkaian dan mengawal penggunaan sumber; (d) Menyelia dan membuat proses *backup server;* (e) Memberi bantuan dalam menyelesaikan masalah-masalah yang dilaporkan oleh pengguna ICT; (f) Menjalankan pengurusan risiko terhadap ancaman keselamatan rangkaian ICT; (g) Menjalankan audit dalaman, mengkaji semula dan melaksanakan proses pengurusan insiden keselamatan siber; dan (h) Melaporkan sebarang insiden keselamatan siber kepada	Pentadbir Rangkaian ICT

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

	CSIRT KPWKM.	
020112 Pengguna		**Peranan**
	Pengguna adalah warga KPWKM dan Agensi yang menggunakan perkhidmatan ICT dan mempunyai peranan seperti berikut: (a) Polisi Keselamatan Siber hendaklah dibaca, difahami dan dipatuhi; (b) Penjagaan kerahsiaan maklumat Kerajaan yang meliputi maklumat rahsia rasmi terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; (c) Penjagaan kerahsiaan kata laluan; (d) Maklumat berkaitan hendaklah tepat dan lengkap dari semasa ke semasa; (e) Penjagaan kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum; (f) Memastikan pihak ketiga mematuhi semua syarat keselamatan yang dinyatakan dengan jelas dalam perjanjian. Perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: i. Polisi Keselamatan Siber KPWKM; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Mematuhi kehendak undang-undang lain yang sedang berkuat kuasa. (g) Tapisan keselamatan dilaksanakan sekiranya dikehendaki berurusan dengan maklumat rasmi rahsia rasmi; (h) Pelaksanaan prinsip-prinsip Polisi Keselamatan Siber dan menjaga kerahsiaan maklumat; (i) Pelaporan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;	Semua Pengguna

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

	(j) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (k) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber KPWKM, Agensi dan Pihak Ketiga/Kontraktor sebagaimana **Lampiran 1**.	
020113 Pihak Ketiga		**Peranan**
	Polisi Keselamatan Siber hendaklah dibaca, difahami dan dipatuhi; (a) Penjagaan kerahsiaan maklumat Kerajaan yang meliputi maklumat rahsia rasmi terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; (b) Penjagaan kerahsiaan kata laluan; (c) Maklumat berkaitan hendaklah tepat dan lengkap dari semasa ke semasa; (d) Penjagaan kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum; (e) Mengetahui dan memahami implikasi keselamatan ICT kesan daripada tindakannya; (f) Pihak Ketiga yang menggunakan perkhidmatan ICT merangkumi semua akses kepada sistem atau maklumat sistem tanpa mengira lokasi pihak ketiga tersebut dan mempunyai peranan seperti berikut: (g) i. Tapisan keselamatan dilaksanakan sekiranya dikehendaki berurusan dengan maklumat rasmi rahsia rasmi; ii. Pelaksanaan prinsip-prinsip Polisi Keselamatan Siber dan menjaga kerahsiaan maklumat; dan iii. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber KPWKM, Agensi dan Pihak Ketiga/Kontraktor sebagaimana **Lampiran 1.**	Pihak Ketiga

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

	020114 Pasukan Tindak Balas Insiden Keselamatan Siber (CSIRT) KPWKM	Peranan
	Keanggotaan Pasukan Tindak Balas Insiden Keselamatan Siber (CSIRT) adalah seperti berikut: **Pengarah :** CDO KPWKM atau Agensi **Pengurus :** ICTSO KPWKM atau Agensi **Ahli CSIRT :** 1. Semua Ketua Unit ICT di KPWKM atau Agensi; 2. Pentadbir Sistem Aplikasi; 3. Pentadbir Keselamatan yang dilantik; 4. Pentadbir Rangkaian yang dilantik; 5. Pentadbir Server yang dilantik; 6. Pentadbir Laman Web yang dilantik; 7. Pentadbir emel yang dilantik; 8. Pentadbir Pangkalan Data yang dilantik; 9. Pentadbir Pusat Data yang dilantik; 10. Pentadbir Aset ICT yang dilantik. Peranan dan tanggungjawab Pasukan Tindak Balas Insiden Keselamatan Siber (CSIRT) adalah seperti berikut: (a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden keselamatan siber; (b) Merekod dan menjalankan siasatan awal insiden keselamatan siber yang diterima; (c) Menangani tindak balas (*response*) insiden keselamatan siber dan mengambil tindakan baik pulih minimum; (d) Menasihati KPWKM dan Agensi mengambil tindakan pemulihan dan pengukuhan; (e) Menyebarkan maklumat berkaitan pengukuhan keselamatan ICT kepada KPWKM dan Agensi; dan (f) Melapor insiden keselamatan siber yang berlaku kepada NACSA sama ada sebagai input atau untuk tindakan seterusnya.	CSIRT KPWKM

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

020115 Pemilik Risiko		**Peranan**
	Pemilik Risiko berperanan dalam proses Penilaian dan Penguraian Risiko berkaitan keselamatan ICT merangkumi tugas-tugas berikut: (a) Mencadangkan cadangan tindakan ke atas risiko yang dikenal pasti; (b) Mengesahkan Pelan Penguraian Risiko; dan (c) Menerima risiko berbaki selepas perlaksanaan Pelan Penguraian Risiko.	Pemilik Risiko
020116 Pengasingan Tugas dan Tanggungjawab		**Peranan**
	Perkara-perkara berikut hendaklah dipatuhi: (a) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat rahsia rasmi atau dimanipulasi.	Pengurus ICT dan ICTSO
020117 Hubungan dengan Pihak Berkuasa dan *Interest Group*		**Peranan**
	KPWKM dan Agensi hendaklah sentiasa berhubung dengan pihak berkuasa yang berkaitan dan *interest group* untuk memastikan organisasi sentiasa dikemaskinikan dengan maklumat berkaitan keselamatan maklumat dan juga operasi.	Warga KPWKM dan Agensi (Mengikut bidang kepakaran)

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

020118 Keselamatan Maklumat dalam Pengurusan Projek		**Peranan**
	Ini bertujuan memastikan keselamatan maklumat dititikberatkan dalam pengurusan projek tanpa mengira jenis projek yang dilaksanakan. Proses ini merangkumi fasa sebelum, semasa dan selepas pelaksanaan projek. Pengurusan Projek ICT merupakan satu pengurusan proses dan prosedur dalam satu tempoh masa, sumber dan tahap kualiti yang ditetapkan bagi menghasilkan satu atau lebih produk ICT. Keselamatan maklumat perlu diambil kira dalam pengurusan projek bagi melindungi maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan objektif keselamatan maklumat dimasukkan di dalam objektif projek; (b) Melaksanakan penilaian risiko keselamatan maklumat di peringkat awal pelaksanaan projek bagi menentukan kaedah kawalan yang bersesuaian; (c) Memastikan keperluan keselamatan maklumat ditangani dari peringkat awal pelaksanaan projek dan dilaksanakan pada setiap fasa pembangunan projek; (d) Memastikan implikasi keselamatan maklumat bagi semua projek ditangani secara teratur dan berkesan; dan (e) Memastikan penguraian risiko keselamatan maklumat sentiasa dikaji semula dengan menilai dan menguji keberkesanannya.	Pengurus Projek

0202 Keselamatan Maklumat dalam Perkhidmatan ICT
Objektif
Memastikan keselamatan maklumat dalam perkhidmatan ICT semasa bertugas rasmi.

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

020201 Keperluan Keselamatan Dalam Perkhidmatan ICT		Peranan
	Pihak luaran yang terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT atau pelawat yang mengunjungi KPWKM dan Agensi atas urusan rasmi. Perkara yang perlu dipatuhi: (a) Mengenalpasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut; (b) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga; (c) Akses kepada aset ICT KPWKM dan Agensi perlu berlandaskan perjanjian dan peraturan yang telah ditetapkan; (d) Melaksanakan keselamatan dan menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber KPWKM, Agensi dan Pihak Ketiga/Kontraktor (**Lampiran 1**) serta Perakuan Akta Rahsia Rasmi 1972 bagi perakuan untuk tidak membocorkan sebarang maklumat rasmi yang diperoleh sepanjang berkhidmat dengan KPWKM dan Agensi; dan (e) Pihak luaran kategori pelawat sahaja dikecualikan daripada mematuhi peraturan (a) hingga (d) seperti di atas.	Pengurus ICT, Pentadbir Sistem

BIDANG 03: KESELAMATAN SUMBER MANUSIA

0301 Keselamatan Sumber Manusia Dalam Tugas Harian		
Objektif		
Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan KPWKM dan Agensi, pihak ketiga (Pembekal, Pakar Runding dan lain-lain) memahami tanggungjawab dan peranan masing-masing. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.		
030101 Sebelum Perkhidmatan		**Peranan**
	Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT sebelum perkhidmatan agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT secara bertulis sebelum perkhidmatan; (b) Menjalani tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; (c) Mengisi secara dalam talian Surat Akuan Pematuhan Polisi Keselamatan Siber KPWKM, Agensi dan Pihak Ketiga/Kontraktor seperti di **Lampiran 1**; (d) Menandatangani Perakuan Untuk Ditandatangani oleh Pegawai Awam Berkaitan Dengan Akta Rahsia Rasmi 1972 (Akta 88) seperti di **Lampiran 2;** (e) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan serta mematuhi peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan; dan	

BIDANG 03: KESELAMATAN SUMBER MANUSIA

	(f) Memastikan calon untuk pegawai dan kakitangan KPWKM dan Agensi lulus tapisan keselamatan CGSO. Saringan pihak ketiga hendaklah dilakukan berdasarkan kaedah yang telah dikenalpasti di peringkat KPWKM dan Agensi.	
030102 Dalam Perkhidmatan		**Peranan**
	Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT dalam perkhidmatan agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT secara bertulis semasa perkhidmatan; (b) Memastikan keselamatan aset ICT diurus berdasarkan prosedur dan peraturan yang ditetapkan oleh KPWKM dan Agensi; (c) Menghadiri program kesedaran yang berkaitan mengenai pengurusan keselamatan aset ICT secara berterusan dan sentiasa berusaha meningkatkan kemahiran berkaitan keselamatan siber; (d) Mempunyai kesedaran berkenaan kepentingan menjaga rahsia Kerajaan dalam urusan kerja harian; (e) Mengambil maklum mengenai tindakan disiplin dan/atau undang-undang yang akan dikenakan sekiranya berlaku perlanggaran dengan prosedur dan peraturan ditetapkan oleh KPWKM dan Agensi; (f) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT melalui kursus, latihan teknikal dan medium yang bersesuaian dengan tugas hakiki bagi memastikan setiap kemudahan ICT digunakan dengan tujuan dan cara yang betul demi menjaga keselamatan	

BIDANG 03: KESELAMATAN SUMBER MANUSIA

	maklumat/siber; dan (g) Mematuhi Prosedur Pengurusan Peralatan ICT yang sedang berkuat kuasa.	
030103 Bertukar atau Tamat Perkhidmatan		**Peranan**
	Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT sebelum bertukar atau tamat perkhidmatan agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT secara bertulis selepas perkhidmatan; (b) Memastikan semua aset ICT dikembalikan kepada KPWKM dan Agensi mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (c) Memastikan kebenaran capaian ke atas maklumat dan kemudahan proses maklumat dibatalkan atau ditarik balik dengan serta-merta mengikut peraturan yang ditetapkan oleh KPWKM dan Agensi; (d) Melaksanakan perakuan bagi melupuskan semua maklumat terperingkat dalam simpanan secara selamat; (e) Mematuhi Prosedur Pengurusan Aset ICT Bagi Pegawai KPWKM dan Agensi yang bertukar keluar, bersara, berhenti kerja atau bercuti panjang; dan Mematuhi Prosedur Pengurusan Peralatan ICT yang sedang berkuat kuasa.	

BIDANG 04: PENGURUSAN ASET

0401 Akauntabiliti Aset		
Objektif		
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT.		
040101 Aset ICT		**Peranan**
	Semua aset ICT hendaklah diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara-perkara seperti berikut hendaklah dipatuhi: (a) Semua maklumat aset ICT hendaklah dikenal pasti dan direkod dalam borang daftar harta modal dan inventori serta sentiasa dikemas kini; (b) Pengurusan aset ICT hendaklah mematuhi pekeliling yang sedang berkuat kuasa; (c) Semua aset ICT hendaklah mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (d) Semua pengguna hendaklah mengesahkan penempatan aset ICT yang ditempatkan di KPWKM dan Agensi; (e) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; (f) Semua pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya dan penggunaan aset hanya untuk tujuan yang dibenarkan sahaja; dan (g) Semua pengguna hendaklah memulangkan semua aset kepada KPWKM dan Agensi selepas penamatan pekerjaan, kontrak atau perjanjian.	Pentadbir Sistem ICT, Pegawai Aset, Penolong Pegawai Aset dan Semua pengguna

BIDANG 04: PENGURUSAN ASET

0402 Pengelasan dan Pengendalian Maklumat		
Objektif		
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
040201 Pengelasan Maklumat		**Peranan**
	Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan yang sedang berkuat kuasa seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad. Maklumat yang tidak diklasifikasikan sebagai maklumat rahsia rasmi boleh diklasifikasikan sebagai terbuka.	Semua Pengguna
040202 Pelabelan Maklumat		**Peranan**
	Maklumat hendaklah dilabel dan dikendali berasaskan peringkat keselamatan yang dikenal pasti selaras dengan peraturan prosedur yang ditetapkan oleh Kerajaan.	Semua Pengguna

BIDANG 04: PENGURUSAN ASET

040203 Pengendalian Maklumat		Peranan
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Pendedahan maklumat kepada pihak yang tidak dibenarkan adalah dilarang; (b) Maklumat hendaklah diperiksa dan dipastikan tepat serta lengkap dari semasa ke semasa; (c) Ketersediaan maklumat hendaklah dipastikan sebelum digunakan; (d) Kerahsiaan kata laluan hendaklah dipatuhi; (e) Standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan hendaklah dipatuhi; (f) Maklumat rahsia rasmi hendaklah diberi perhatian terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan; (g) Kerahsiaan langkah-langkah keselamatan ICT hendaklah dijaga daripada pengetahuan umum; dan (h) Prosedur pengendalian aset hendaklah mematuhi garis panduan/ pekeliling yang sedang berkuat kuasa. (i) Maklumat rahsia rasmi KPWKM dan Agensi yang disimpan secara fizikal atau elektronik tidak boleh disimpan melebihi tempoh yang ditetapkan. (j) Maklumat rahsia rasmi KPWKM dan Agensi hendaklah dilupuskan dengan kaedah yang selamat apabila tidak lagi diperlukan. Ini adalah untuk mengelakkan daripada pendedahan maklumat rasmi Kerajaan dan maklumat sensitif seperti PII kepada pihak yang tidak dibenarkan. (k) KPWKM dan Agensi di bawah KPWKM hendaklah memastikan rekod pelupusan disimpan sebagai bukti.	Semua Pengguna

BIDANG 04: PENGURUSAN ASET

040204 Pencegahan Kebocoran Data		Peranan
	Pencegahan Kebocoran Data *(Data Leakage Prevention)* bertujuan untuk mengesan dan mencegah kebocoran dan pengeluaran maklumat atau data yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti dan mengelaskan maklumat sensitif untuk melindunginya daripada kebocoran seperti maklumat peribadi, model harga dan reka bentuk; (b) Memantau saluran-saluran kebocoran data seperti e-mel, pemindahan fail, peranti mudah alih dan peranti storan mudah alih; (c) Mengambil tindakan untuk mencegah kebocoran maklumat contohnya menahan e-mel yang mengandungi maklumat sensitif; (d) Melaksanakan program kesedaran kepada warga KPWKM dan Agensi sebagai langkah pencegahan bagi kebocoran data.	

BIDANG 04: PENGURUSAN ASET

0403 Pengurusan Media Storan	
Objektif	
Melindungi media daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
040301 Prosedur Pengendalian Media Storan	**Peranan**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket dan cakera padat. Peraturan yang perlu dipatuhi dalam pengurusan media storan adalah berdasarkan Arahan Keselamatan 1985 dan seperti berikut: (a) Media mudah alih hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media mudah alih hendaklah terhad kepada Pentadbir dan pegawai yang dibenarkan sahaja; (c) Media mudah alih perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di tempat yang mempunyai ciri-ciri keselamatan dengan mengikut prosedur yang ditetapkan; (e) Akses dan pergerakan media mudah alih hendaklah direkodkan; (f) Perkakasan backup hendaklah diletakkan di tempat yang terkawal; (g) Mengadakan salinan atau backup pada media storan kedua bagi tujuan keselamatan dan mengelakkan kehilangan data. Media storan kedua hendaklah	Semua Pengguna

BIDANG 04: PENGURUSAN ASET

	disimpan di tempat yang selamat; Hanya maklumat rasmi dibenarkan untuk disimpan dalam media storan yang dibekalkan oleh KPWKM dan Agensi.	

BIDANG 04: PENGURUSAN ASET

040302 Pelupusan Media Storan		**Peranan**
	Semua maklumat dalam media storan yang hendak dilupuskan mestilah dihapuskan terlebih dahulu. Proses pelupusan hendaklah dilakukan dengan teratur dan selamat mengikut prosedur pelupusan.	Semua Pengguna
040303 Penghantaran dan Pemindahan Media Storan		**Peranan**
	Peraturan yang perlu dipatuhi dalam penghantaran dan pemindahan media adalah berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017) dan adalah seperti berikut: (a) Penghantaran dan pemindahan media storan ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu serta direkodkan; dan (b) Memastikan media storan yang mengandungi maklumat rahsia rasmi dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa proses pemindahan.	Semua Pengguna

BIDANG 04: PENGURUSAN ASET

040304 Peralatan Media Mudah Alih Persendirian (*Bring Your Own Device (BYOD)*)		**Peranan**
	Penggunaan BYOD yang disambungkan kepada rangkaian Kementerian dan Agensi sama ada menyimpan atau mengakses data rasmi Kerajaan adalah tertakluk kepada keperluan dan kawalan penggunaan BYOD. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna perlu mengetahui risiko dan kesan penggunaan BYOD terhadap keselamatan maklumat; (b) Pengguna perlu mengetahui peraturan-peraturan yang telah ditetapkan apabila menggunakan BYOD; (c) Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan siber yang berpunca daripada penggunaan BYOD; (d) Pendaftaran ke atas peralatan mudah alih; (e) Keperluan ke atas perlindungan secara fizikal; (f) Kawalan ke atas pemasangan perisian peralatan mudah alih; (g) Kawalan ke atas versi dan patches perisian; (h) Kawalan terhadap kod perosak; (i) Sekatan ke atas akses perkhidmatan maklumat secara dalam talian; (j) Kawalan perkhidmatan maklumat secara kawalan akses atau teknik kriptografi; dan (k) Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan. (l) Semua maklumat rasmi kerajaan adalah hak milik Kerajaan; (m) Sebarang bahan rasmi yang dimuat naik/ edar/ kongsi hendaklah mendapat kebenaran Ketua Pengarah dan Pengarah Negeri; (n) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber dan Akta Rahsia Rasmi 1972 [Akta 88];	Semua Pengguna

BIDANG 04: PENGURUSAN ASET

	(o) Memastikan peranti yang digunakan mempunyai kawalan keselamatan seperti berikut:	
	i. Menetapkan mekanisme kawalan akses bagi BYOD dan akan mengunci secara automatik apabila tidak digunakan; ii. Melaksanakan enkripsi dan/atau perlindungan ke atas folder yang mempunyai maklumat rasmi Kerajaan yang disimpan di dalam peranti BYOD; dan iii. Memastikan BYOD mempunyai ciri-ciri keselamatan standard seperti antivirus, *patching* terkini dan *anti theft*. (p) Pengguna adalah dilarang daripada melakukan perkara berikut: i. Menyimpan maklumat rasmi yang sensitif dan rahsia rasmi di dalam BYOD; ii. Menggunakan BYOD untuk mengakses, menyimpan dan menyebarkan maklumat rasmi yang sensitif dan rahsia rasmi; iii. Menjadikan BYOD sebagai medium sandaran (*backup*) bagi maklumat rasmi; iv. Merakam komunikasi dan dokumen rasmi untuk tujuan peribadi; dan v. Menjadikan BYOD sebagai *access point* kepada aset ICT KPWKM dan Agensi untuk capaian ke Internet tanpa kebenaran.	

BIDANG 04: PENGURUSAN ASET

	(q) Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD seperti berikut: i. Semua maklumat rasmi kerajaan adalah hak milik Kerajaan; ii. Sebarang bahan rasmi yang dimuat naik/ edar/ kongsi hendaklah mendapat kebenaran Ketua Pengarah dan Pengarah Negeri; dan iii. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber dan Akta Rahsia Rasmi 1972 [Akta 88]. (r) Pengguna adalah tertakluk kepada perkara seperti berikut: i. Memadamkan segala maklumat yang berkaitan dengan urusan rasmi KPWKM dan Agensi sekiranya bertukar/ditamatkan perkhidmatan/bersara atau sewaktu dihantar ke pusat servis untuk penyelenggaraan; ii. Bertanggungjawab dan boleh dikenakan tindakan tatatertib atau tindakan undang-undang sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/ kerosakan/ pendedahan maklumat rasmi Kerajaan; iii. KPWKM dan Agensi berhak merampas mana-mana BYOD pengguna sekiranya didapati atau disyaki tidak mematuhi peraturan yang telah ditetapkan atau untuk tujuan siasatan; iv. KPWKM dan Agensi tidak bertanggungjawab atas kehilangan, kerosakan data atau aplikasi dalam BYOD yang digunakan; dan v. Membenarkan pihak Kerajaan untuk membuat analisa risiko ke atas BYOD yang digunakan.	

BIDANG 05: KAWALAN CAPAIAN

0501 Dasar Kawalan Capaian		
Objektif		
Mengawal capaian ke atas maklumat.		
050101 Keperluan Kawalan Capaian		**Peranan**
	Capaian kepada aset, proses, maklumat dan rangkaian hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia hendaklah direkod, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumen dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara berikut hendaklah dipatuhi: (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; (d) Kawalan ke atas kemudahan pemprosesan maklumat. (e) Kawalan ke atas capaian aplikasi; dan (f) Kawalan kebenaran untuk menyebarkan maklumat.	Bahagian / Unit ICT KPWKM dan Agensi dan ICTSO

BIDANG 05: KAWALAN CAPAIAN

0502 Pengurusan Capaian Pengguna		
Objektif		
Mengawal capaian pengguna ke atas aset ICT.		
050201 Akaun Pengguna		**Peranan**
	Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh KPWKM dan Agensi sahaja boleh digunakan; (b) Pengwujudan dan pembatalan mesti dibuat melalui proses rasmi yang disahkan oleh pegawai yang bertanggungjawab; (c) Akaun pengguna mestilah unik berdasarkan identiti pengguna; (d) Tahap capaian adalah berdasarkan kepada keperluan skop tugasan yang ditetapkan. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (e) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan KPWKM. Akaun boleh dibatalkan jika penggunaannya melanggar peraturan yang terpakai di KPWKM dan Agensi; (f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (g) Pentadbir Sistem ICT hendaklah melakukan semakan akaun pengguna sekurang-kurangnya dua kali setahun untuk memastikan hanya akaun pengguna yang sah dan aktif sahaja dikekalkan dalam sistem;	Semua Pengguna dan Pentadbir Sistem ICT

BIDANG 05: KAWALAN CAPAIAN

	(h) Pentadbir Sistem ICT boleh menyahaktifkan (*disable/inactive*) akaun pengguna dengan kelulusan sekiranya pengguna bercuti panjang dalam tempoh waktu melebihi 30 hari; dan (i) Pentadbir Sistem ICT juga boleh menamatkan akaun pengguna dengan kelulusan di atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan.	
050202 Hak Capaian		**Peranan**
	Hak capaian kepada aset ICT dan maklumat hendaklah dikawal melalui proses peruntukan hak capaian pengguna, kajian semula hak capaian pengguna dan penyelarasan hak capaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peruntukan untuk memberi atau membatalkan hak capaian pengguna perlu mendapat kebenaran daripada pemilik sistem; (b) Hak capaian pengguna perlu disemak dan dikemaskini secara berkala berdasarkan peranan dan tanggungjawab pengguna; (c) Hak capaian pengguna perlu ditamatkan atau dibuat pelarasan apabila tamat perkhidmatan, bertukar, berpindah atau terdapat perubahan.	Pentadbir Sistem ICT

BIDANG 05: KAWALAN CAPAIAN

050203 Pengurusan Kata Laluan		**Peranan**
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KPWKM dan Agensi seperti berikut: (a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Kata laluan hendaklah ditukar apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara alfanumerik dengan gabungan aksara (huruf besar), aksara (huruf kecil), angka (nombor) dan aksara khusus (simbol); (d) Kata laluan **TIDAK BOLEH** didedahkan dengan apa cara sekalipun; (e) Kata laluan windows dan screen saver hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa login; (g) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (i) Kata laluan hendaklah ditukar selepas 90 hari; (j) Tidak dibenarkan penggunaan semula tiga (3) kata laluan yang terakhir digunakan. (k) Penggunaan Multifactor Authentication (MFA) adalah digalakkan bagi sistem dan aplikasi di KPWKM dan Agensi; dan (l) Pengguna disarankan untuk tidak menggunakan fungsi remember me bagi kata laluan.	Semua Pengguna dan Pentadbir Sistem ICT

BIDANG 05: KAWALAN CAPAIAN

0503 Kawalan Capaian Rangkaian		
Objektif		
Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.		
050301 Capaian Rangkaian		**Peranan**
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dan mematuhi perkara-perkara berikut : (a) Peranti keselamatan yang bersesuaian hendaklah dipasang atau ditempatkan di antara rangkaian KPWKM dan Agensi; dan rangkaian awam; (b) Mekanisme pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya hendaklah diwujud dan dikuat kuasakan; (c) Kawalan capaian pengguna hendaklah dikuat kuasa dan dipantau terhadap perkhidmatan rangkaian ICT ; dan (d) Untuk capaian di luar rangkaian KPWKM dan Agensi, komunikasi dari jarak jauh untuk mengendalikan sistem di dalam Pusat Data mestilah menggunakan *Virtual Private Network* (VPN).	Pentadbir Rangkaian ICT dan ICTSO
050302 Capaian Internet		**Peranan**
	Perkara-perkara berikut hendaklah dipatuhi : (a) Penggunaan Internet di KPWKM dan Agensi hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja dan melindungi kemasukan *malicious code*, virus dan bahan- bahan yang tidak sepatutnya ke dalam rangkaian KPWKM dan Agensi; dan (b) Kaedah *Content Filtering* hendaklah digunakan bagi mengawal akses internet mengikut fungsi kerja dan	Pentadbir Rangkaian ICT

BIDANG 05: KAWALAN CAPAIAN

	pemantauan tahap pematuhan.	

BIDANG 05: KAWALAN CAPAIAN

0503 Kawalan Capaian Rangkaian		
Objektif		
Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.		
050301 Capaian Rangkaian		**Peranan**
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dan mematuhi perkara-perkara berikut : (a) Peranti keselamatan yang bersesuaian hendaklah dipasang atau ditempatkan di antara rangkaian KPWKM dan Agensi; dan rangkaian awam; (b) Mekanisme pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya hendaklah diwujud dan dikuat kuasakan; (c) Kawalan capaian pengguna hendaklah dikuat kuasa dan dipantau terhadap perkhidmatan rangkaian ICT ; dan (d) Untuk capaian di luar rangkaian KPWKM dan Agensi, komunikasi dari jarak jauh untuk mengendalikan sistem di dalam Pusat Data mestilah menggunakan *Virtual Private Network* (VPN).	Pentadbir Rangkaian ICT dan ICTSO
050302 Capaian Internet		**Peranan**
	Perkara-perkara berikut hendaklah dipatuhi : (a) Penggunaan Internet di KPWKM dan Agensi hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja dan melindungi kemasukan *malicious code*, virus dan bahan- bahan yang tidak sepatutnya ke dalam rangkaian KPWKM dan Agensi; (b) Kaedah *Content Filtering* hendaklah digunakan bagi mengawal akses internet mengikut fungsi kerja dan	Pentadbir Rangkaian ICT

BIDANG 05: KAWALAN CAPAIAN

	pemantauan tahap pematuhan;	

BIDANG 05: KAWALAN CAPAIAN

	(c) Penggunaan teknologi *bandwidth management* untuk mengawal aktiviti seperti *video conferencing, video streaming, chat, downloading* adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; (d) Penggunaan internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya; (e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh KPWKM dan Agensi; (f) Bahan yang diperoleh dari internet hendaklah dipastikan ketepatan dan kesahihannya. Sebagai amalan terbaik, sekiranya rujukan sumber internet digunakan sebagai rujukan ia hendaklah dinyatakan; (g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian / Unit sebelum dimuat naik ke internet; (h) Kakitangan KPWKM dan Agensi hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; (i) Sebarang bahan yang dimuat turun dari internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KPWKM dan Agensi; (j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mematuhi peraturan dan etika perkhidmatan awam. Penggunaan *modem /mobile broadband* untuk tujuan sambungan ke internet tidak dibenarkan kecuali setelah mendapat kebenaran daripada Pengurus ICT; dan	

BIDANG 05: KAWALAN CAPAIAN

	(k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video dan lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah dan melanggar etika penjawat awam. Penggunaan media sosial hendaklah dikawal dan dipastikan mematuhi garis panduan penggunaan media sosial yang sedang berkuat kuasa.	

BIDANG 05: KAWALAN CAPAIAN

0504 Kawalan Capaian Sistem Pengoperasian		
Objektif		
Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.		
050401 Capaian Sistem Pengoperasian		**Peranan**
	Kawalan capaian sistem pengoperasian perlu bagi mengelak sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi hendaklah digunakan untuk menghalang capaian kepada sumber sistem komputer. Kemudahan ini juga perlu bagi: (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (b) Merekod capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan kakitangan KPWKM dan Agensi yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan; (c) Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem. Perkara-perkara berikut hendaklah dipatuhi: (a) Kawalan capaian ke atas sistem pengoperasian hendaklah dikawal menggunakan prosedur *log-on* yang terjamin;	Pentadbir Sistem ICT dan ICTSO

BIDANG 05: KAWALAN CAPAIAN

	(b) Satu pengenalan diri (ID) yang unik hendaklah diwujudkan untuk setiap kakitangan KPWKM dan Agensi; dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Penggunaan program/aplikasi hendaklah dikawal dan dihadkan; dan (d) Tempoh sambungan ke sesebuah aplikasi berisiko tinggi hendaklah dihadkan.	

BIDANG 05: KAWALAN CAPAIAN

050402 Kad Pintar / Token (GPKI)		**Peranan**
	Perkara-perkara berikut hendaklah dipatuhi : (a) Penggunaan Kad Pintar / Token (GPKI) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; (b) Kad Pintar / Token (GPKI) hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian Kad Pintar / Token (GPKI) untuk sebarang capaian sistem adalah tidak dibenarkan. Kad / Token (GPKI) yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan (d) Sebarang kehilangan, kerosakan dan kata laluan disekat hendaklah dimaklumkan kepada Bahagian / Unit Kewangan.	Semua Pengguna

BIDANG 05: KAWALAN CAPAIAN

0505 Kawalan Capaian Sistem Aplikasi dan Maklumat		
Objektif		
Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem aplikasi.		
050501 Capaian Sistem Aplikasi dan Maklumat		**Peranan**
	Bertujuan melindungi sistem aplikasi dan maklumat sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan penyalahgunaan dan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara- perkara berikut hendaklah dipatuhi: (a) Kakitangan KPWKM dan Agensi hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (c) Capaian sistem dan aplikasi hendaklah dihadkan kepada tiga (3) kali percubaan sahaja. Sekiranya gagal, akaun pengguna akan disekat; (d) Kawalan sistem rangkaian hendaklah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah. Untuk capaian di luar rangkaian KPWKM dan Agensi, komunikasi dari jarak jauh untuk mengendalikan sistem di dalam Pusat Data mestilah menggunakan *Virtual Private Network (VPN)*; dan (e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem ICT dan ICTSO

BIDANG 05: KAWALAN CAPAIAN

050502 Prosedur *Secure Log-On*		**Peranan**
	KPWKM dan Agensi hendaklah mengenal pasti teknik pengesahan *log-on* yang sesuai seperti berikut: (a) Tidak memaparkan sistem atau aplikasi selagi proses *log-on* tidak berjaya; (b) Paparkan suatu notis amaran bahawa komputer hanya boleh diakses oleh pengguna yang sah; (c) Tidak memberikan bantuan mesej semasa prosedur *log-on*; (d) Pengesahan *log-on;* (e) Perlindungan terhadap *Brute Force log-on*; (f) Log "aktiviti *log-on*" yang berjaya dan tidak berjaya; (g) Mengadakan amaran keselamatan jika ada potensi percubaan atau pencerobohan *log-on* berjaya dikesan; (h) Memaparkan maklumat berikut setelah selesai *log-on* yang berjaya: i. Tarikh dan masa *log-on* sebelumnya; dan ii. butir-butir percubaan *log-on* yang tidak berjaya (j) Tidak memaparkan kata laluan; (k) Tidak menghantar kata laluan dalam "*clear-text*" melalui rangkaian; (l) Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu; dan (m) Menghadkan sesi sambungan sekatan untuk aplikasi yang berisiko tinggi.	Pentadbir Sistem ICT dan ICTSO

BIDANG 05: KAWALAN CAPAIAN

050503 Penggunaan Sistem Fasiliti		**Peranan**
	Penggunaan perisian utiliti yang berupaya melaksanakan *Overriding System* hendaklah mendapat kelulusan, dikawal dan dipantau.	Pentadbir Sistem ICT dan ICTSO

BIDANG 05: KAWALAN CAPAIAN

050504 Pengurusan Kod Sumber (*Source Code*)		**Peranan**
	Pembangunan perisian secara dalaman (*inhouse)* atau sumber luar (*outsource)* hendaklah diselia dan dipantau oleh KPWKM dan Agensi dengan mengambil kira perkara- perkara berikut: (a) Kakitangan sokongan KPWKM dan Agensi hendaklah dihadkan akses kepada kod sumber (*source code);* (b) Log audit hendaklah dikekalkan bagi semua akses kepada kod sumber; (c) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada prosedur kawalan perubahan yang ketat; dan (d) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik Kerajaan.	Pentadbir Sistem ICT dan ICTSO

BIDANG 06: KRIPTOGRAFI

0601 Kawalan Kriptografi		
Objektif		
Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.		
060101 Enkripsi		**Peranan**
	Enkripsi/penyulitan digunakan untuk melindungi kerahsiaan, integriti dan kesahihan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap maklumat rahsia rasmi hendaklah disulitkan; (b) Penggunaan Produk Kriptografi Terpercaya untuk mengendalikan Maklumat Rasmi adalah digalakkan; dan (c) Kesemua pelaksanaan sistem hendaklah menggunakan ID dan kata laluan atau dibuat enkripsi.	Pemilik Sistem, Pentadbir Sistem Aplikasi, Pengguna
060102 Tandatangan Digital		**Peranan**
	Semua transaksi maklumat rahsia rasmi secara elektronik hendaklah menggunakan tandatangan digital.	Pemilik Sistem, Pentadbir Sistem ICT KPWKM dan Agensi serta Pengguna

BIDANG 06: KRIPTOGRAFI

060103 Pengurusan Infrastruktur Kunci Awam (PKI) - jika refer pekeliling PPPA Bil 4 Tahun 2025 - Perkhidmatan Prasarana Kunci Awam		**Peranan**
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut; (b) Memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi diguna pakai di KPWKM dan Agensi; (c) Setiap urusan transaksi maklumat sensitif hendaklah menggunakan kunci kriptografi supaya mendapat perlindungan dan pengiktirafan undang- undang; dan (d) Sebarang perubahan kepada pemilik / pemegang kunci hendaklah dilaporkan kepada Pentadbir Sistem.	Pemilik Sistem, Pentadbir Sistem Aplikasi, Pengguna

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Keselamatan Kawasan		
Objektif		
Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.		
070101 Perimeter Keselamatan Fizikal		**Peranan**
	Perimeter keselamatan fizikal adalah bertujuan untuk menghalang akses tanpa kebenaran, kerosakan dan gangguan secara fizikal terhadap premis, aset ICT dan maklumat KPWKM dan Agensi. (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan kekuatan setiap perimeter perlu bergantung kepada keperluan keselamatan aset dalam perimeter dan hasil penilaian risiko; (b) Perimeter bangunan atau tapak yang mengandungi maklumat dan kemudahan pemprosesan maklumat perlu kukuh secara fizikal dan semua pintu dan tingkap perlu dilindungi sewajarnya daripada akses tanpa kebenaran; (c) Memasang alat penggera dan kamera litar tertutup; (d) Mengehadkan laluan 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 yang diberi kebenaran sahaja boleh melalui pintu masuk ini. Kawalan masuk fizikal bertujuan mengawal akses Pengguna, Pembekal	Setiausaha Bahagian Khidmat Pengurusan KPWKM dan Agensi

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

	dan Pihak Ketiga bagi keselamatan maklumat organisasi seperti berikut: i. Setiap kakitangan KPWKM dan Agensi hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; ii. Semua kad pengenalan KPWKM dan Agensi hendaklah diserahkan balik kepada Bahagian Khidmat Pengurusan apabila kakitangan KPWKM dan Agensi berhenti, bersara atau bertukar; iii. Setiap pelawat hendaklah mendapatkan Pas Pelawat di pintu kawalan utama premis KPWKM dan Agensi. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan iv. Pihak Ketiga hendaklah menyerahkan semula pas pelawat kepada KPWKM dan Agensi apabila urusan selesai atau tamat kontrak; v. Mereka bentuk dan melaksanakan keselamatan fizikal di pejabat, bilik dan kemudahan infrastruktur; vi. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, dan sebarang bencana; vii. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan viii. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

070102 Kawalan Masuk Fizikal		**Peranan**
	Kawalan masuk fizikal bertujuan mengawal akses oleh Pengguna, Pembekal dan Pihak Ketiga bagi keselamatan maklumat organisasi. (a) Setiap kakitangan KPWKM dan Agensi hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua kad pengenalan KPWKM dan Agensi hendaklah diserahkan balik kepada Bahagian Khidmat Pengurusan apabila kakitangan KPWKM dan Agensi berhenti ,bersara atau bertukar; (c) Setiap pelawat hendaklah mendapatkan Pas Pelawat di pintu kawalan utama premis KPWKM dan Agensi. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Pihak Ketiga hendaklah menyerahkan semula pas pelawat kepada KPWKM dan Agensi apabila urusan selesai atau tamat kontrak.	Semua Pengguna dan Bahagian Pentadbiran KPWKM dan Agensi
070103 Kawalan Pejabat, Bilik dan Kemudahan ICT		**Peranan**
	Keselamatan fizikal untuk pejabat, bilik dan kemudahan ICT perlu direka bentuk dan dilaksanakan bagi melindungi daripada pencerobohan. (a) Kawasan pejabat, bilik dan kawasan yang menempatkan kemudahan ICT hanya boleh diakses oleh pihak yang dibenarkan sahaja; dan (b) Penunjuk ke lokasi bilik operasi dan kawasan larangan tidak harus menonjol dan hanya memberi petunjuk minimum.	Setiausaha Bahagian Khidmat Pengurusan/ Bahagian Pengurusan Maklumat

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

070104 Perlindungan Daripada Ancaman Luaran dan Dalaman		**Peranan**
	KPWKM dan Agensi hendaklah mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, gangguan awam dan bencana.	Ketua Setiausaha KPWKM dan Ketua Pengarah Agensi dan ICTSO
070105 Bekerja di Kawasan Selamat		**Peranan**
	Kawasan selamat ialah kawasan larangan yang dihadkan kemasukan kepada pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset dan maklumat ICT yang terdapat di kawasan tersebut. Kawasan larangan di KPWKM dan Agensi adalah Pusat Data, Bilik Server, Ruang Kerja ICT, Bilik Fail dan Stor Peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Akses ke kawasan larangan hanyalah kepada pegawai- pegawai yang dibenarkan sahaja; (b) Pembekal adalah dilarang untuk memasuki kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai. Tanda kawasan larangan hendaklah dipamerkan; (c) Pembekal dan pihak ketiga adalah dilarang untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal. Mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai;	Pentadbir Sistem ICT, Pentadbir Rangkaian, Pentadbir Aplikasi, Pembekal, Pihak Ketiga dan Pelawat

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

	(d) Pelawat yang ingin memasuki ruang kerja perlu mendapat kebenaran daripada Pengurus ICT; (e) Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk; dan (f) Pengguna KPWKM dan Agensi yang perlu berurusan di pusat data hendaklah mendapatkan kebenaran dan mengisi buku log keluar masuk Pusat Data.	
070106 Kawasan Penghantaran dan Pemunggahan		**Peranan**
	Kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain hendaklah dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	Setiausaha Bahagian Khidmat Pengurusan KPWKM dan Agensi
070107 Pemantauan Keselamatan Fizikal		**Peranan**
	Akses fizikal ke premis hendaklah dikawal dan dipantau setiap masa daripada pihak yang tidak dikenali atau sebarang aktiviti yang mencurigakan. Langkah-langkah berikut boleh dipertimbangkan bagi pemantauan keselamatan fizikal: (a) Memastikan premis disediakan dengan sistem pemantauan komprehensif seperti Pengawal Keselamatan, alat penggera pencerobohan, Closed-Circuit Television (CCTV); (b) Sistem pemantauan fizikal hendaklah dilindungi daripada sebarang ancaman yang boleh menjejaskan fungsi atau keselamatan maklumat KPWKM dan Agensi; (c) Sistem pemantauan fizikal hendaklah diselenggara secara berkala bagi memastikan ketersediaan fungsinya semasa kecemasan; dan (d) Tempoh pengekalan rekod pemantauan fizikal adalah	Setiausaha Bahagian Khidmat Pengurusan KPWKM dan Agensi

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

	mengikut keupayaan semasa.	

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

0702 Keselamatan Peralatan		
Objektif		
Melindungi peralatan ICT KPWKM dan Agensi daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan ICT.		
070201 Peralatan ICT		**Peranan**
	Perkara- perkara berikut hendaklah dipatuhi: (a) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain hendaklah diletakkan di dalam rak khas dan berkunci; (b) Semua peralatan ICT yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin atau mempunyai pengudaraan (*air ventilation*) yang sesuai; (c) Pihak KPWKM dan Agensi hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (d) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (e) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT; (f) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pengurus ICT; (g) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;	Semua Pengguna

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

	(h) Pengguna mestilah memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; (i) KPWKM dan Agensi adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (j) KPWKM dan Agensi mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; (k) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (l) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (m) Peralatan-peralatan kritikal hendaklah disokong oleh *Uninterruptable Power Supply* (UPS); (n) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO atau Pegawai Aset dengan segera dan mematuhi prosedur yang sedang berkuat kuasa; (o) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada pekeliling yang sedang berkuat kuasa; (p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada ICTSO atau Pegawai Aset untuk dibaik pulih; (q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan; (r) Dilarang menggunakan kata laluan bagi pentadbir (*administrator password)* atau *default password* yang telah ditetapkan oleh Pentadbir Sistem ICT; (s) Bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (t) Sebarang bentuk penyelewengan atau salah guna	

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

	peralatan ICT hendaklah dilaporkan kepada ICTSO; (u) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan dimatikan (*Off*) apabila meninggalkan pejabat; dan (v) Memastikan plug dicabut daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

070202 Bekalan Utiliti		Peranan
	Bekalan utiliti merupakan semua kemudahan utiliti seperti bekalan elektrik, bekalan air, alat penghawa dingin, saluran kumbahan dan lain-lain yang hendaklah dilindungi daripada kegagalan fungsi atau gangguan. Perkara-perkara berikut hendaklah dipatuhi: (a) Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT. (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal supaya mendapat bekalan kuasa berterusan; (c) Suis kecemasan hendaklah ditempatkan berhampiran laluan kecemasan. Lampu kecemasan perlu disediakan dan berfungsi sekiranya berlaku gangguan bekalan kuasa; (d) Bekalan air hendaklah mencukupi bagi memastikan sistem penghawa dingin berfungsi dengan baik; dan (e) Semua peralatan sokongan bekalan utiliti hendaklah disemak dan diuji secara berjadual.	Bahagian/Unit ICT, KPWKM dan Agensi / Bahagian Khidmat Pengurusan dan ICTSO

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

070203 Keselamatan Kabel		**Peranan**
	Kabel bekalan kuasa, rangkaian dan telekomunikasi hendaklah dilindungi daripada gangguan dan kerosakan. Langkah-langkah keselamatan seperti berikut hendaklah diambil: (a) Menggunakan kabel yang mengikut spesifikasi yang ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* (d) Semua kabel hendaklah dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; dan (e) Memastikan hanya pihak KPWKM, Agensi atau pihak ketiga yang dibenarkan sahaja boleh melaksanakan pemasangan atau penyelenggaraan kabel.	Bahagian/ Unit ICT, KPWKM dan Agensi / Bahagian Khidmat Pengurusan dan ICTSO

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

070204 Penyelenggaraan Perkakasan		**Peranan**
	Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara berikut hendaklah dipatuhi: (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Penyelenggaraan melibatkan perkakasan ICT dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan kepada pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	Pegawai Aset dan Bahagian/ Unit ICT KPWKM dan Agensi

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

070205 Pergerakan Aset		**Peranan**
	Semua perkakasan, maklumat dan perisian yang hendak dibawa keluar hendaklah mendapatkan kelulusan ICTSO atau Pegawai Aset. (a) Peralatan ICT yang hendak dibawa keluar dari premis KPWKM dan Agensi hendaklah mendapat kelulusan ICTSO atau Pegawai Aset serta direkodkan bagi tujuan pemantauan; dan (b) KPWKM dan Agensi tidak dibenarkan mengubah lokasi peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran ICTSO atau Pegawai Aset.	Semua Pengguna
070206 Peralatan di Luar Premis		**Peranan**
	Perkakasan yang dibawa keluar dari premis KPWKM dan Agensi adalah terdedah kepada pelbagai risiko. Perkakasan yang dibawa keluar dari premis KPWKM dan Agensi adalah terdedah kepada pelbagai risiko. Perkara-perkara berikut hendaklah dipatuhi: (a) Memastikan peralatan ICT tersebut direkodkan oleh pegawai yang dilantik ke atas peralatan ICT tersebut; (b) Peralatan ICT tersebut perlu dilindungi dan dikawal sepanjang masa; (c) Penyimpanan atau penempatan peralatan ICT tersebut mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (d) Menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap.	Semua Pengguna

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

070207 Pelupusan dan Penggunaan Semula Perkakasan		Peranan
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KPWKM dan Agensi dan ditempatkan di KPWKM dan Agensi dan semua cawangan di peringkat negeri. Peralatan ICT yang hendak dilupuskan hendaklah melalui prosedur pelupusan semasa. Pelupusan hendaklah dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan KPWKM dan Agensi. Perkara-perkara berikut hendaklah dipatuhi: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; (b) Sekiranya maklumat perlu disimpan, maka kakitangan KPWKM dan Agensi bolehlah membuat penduaan; (c) Memastikan data-data dan perisian berlesen dalam storan peralatan ICT yang hendak dilupuskan telah dihapuskan dengan cara yang selamat; (d) 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 , Bahagian / Unit ICT KPWKM dan Agensi

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

	(e) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset (SPA); (f) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan	

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

	(g) Kakitangan KPWKM dan Agensi adalah DILARANG daripada melakukan perkara- perkara seperti berikut i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan dalaman komputer seperti RAM, *hard disk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti Audio Video Recorder (AVR), speaker dan peralatan yang berkaitan ke mana-mana bahagian di KPWKM dan Agensi; iii. Memindah keluar dari KPWKM dan Agensi mana-mana peralatan ICT yang hendak dilupuskan; dan iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggungjawab Unit Pengurusan Aset KPWKM dan Agensi; (h) Penggunaan semula perkakasan hendaklah mendapat kebenaran daripada pemilik dan hendaklah melalui proses penghapusan maklumat menggunakan kaedah yang bersesuaian bagi mengelakkan kebocoran atau penyalahgunaan maklumat.	

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

070208 Perkakasan Yang Tidak Digunakan		**Peranan**
	Pengguna hendaklah memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara-perkara berikut: (a) Tamatkan sesi aktif apabila selesai tugas; (b) *Log-off* kerangka utama <<kpwkm tidak mempunyai mainframe , pohon delete>>, pelayan dan komputer pejabat apabila sesi bertugas selesai; dan (c) Memastikan komputer atau terminal selamat dan bebas daripada capaian pengguna yang tidak dibenarkan.	Semua Pengguna

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

070209 *Clear Desk & Clear Screen*		**Peranan**
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara berikut hendaklah dipatuhi: (a) Menggunakan kemudahan *password screen saver* atau *Log-out* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas,mesin faksimili dan mesin fotostat.	Semua Pengguna

BIDANG 08: KESELAMATAN OPERASI

0801 Tanggungjawab dan Prosedur Operasi		
Objektif		
Memastikan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman.		
080101 Dokumen Prosedur Operasi		**Peranan**
	Perkara-perkara berikut hendaklah dipatuhi: (a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan; (d) Memastikan hanya pengguna yang dibenarkan sahaja boleh mengakses dokumen prosedur operasi; dan (e) Semua prosedur operasi hendaklah dikemas kini dari semasa ke semasa mengikut keperluan. Semakan semula perlu dilakukan secara berkala.	Semua Pengguna

BIDANG 08: KESELAMATAN OPERASI

080102 Kawalan Perubahan		Peranan
	Perkara-perkara berikut hendaklah dipatuhi: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; dan Aplikasi hendaklah dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan KPWKM dan Agensi; (b) Pegawai yang telah dipertanggungjawabkan dan ditetapkan hendaklah memantau penambahbaikan, pembetulan atau perubahan yang dilakukan oleh pihak ketiga; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;	Pemilik Sistem, Pentadbir Sistem Aplikasi

BIDANG 08: KESELAMATAN OPERASI

	(d) Akses kepada kod sumber (source code) aplikasi hendaklah dihadkan kepada pengguna yang dibenarkan; (e) Permohonan perubahan hendaklah diluluskan oleh Jawatankuasa atau Pegawai yang diberikan kuasa melulus di peringkat KPWKM dan Agensi; dan (f) Permohonan perubahan hendaklah diluluskan oleh Jawatankuasa atau Pegawai yang diberikan kuasa melulus di peringkat KPWKM dan Agensi.	
080103 Pengurusan Kapasiti		**Peranan**
	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. Keperluan kapasiti ini juga hendaklah mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT dan ICTSO

BIDANG 08: KESELAMATAN OPERASI

080104 Pengasingan Persekitaran Pembangunan, Pengujian, Latihan dan Operasi		**Peranan**
	Persekitaran pembangunan, pengujian dan operasi perlu diasingkan bagi mengurangkan risiko akses tanpa izin atau perubahan kepada persekitaran operasi.	Pemilik Sistem ICT dan Pengurus ICT
080105 Pengurusan Konfigurasi		**Peranan**
	Konfigurasi keselamatan perkakasan, perisian, perkhidmatan(contoh pengkomputeran awan) dan rangkaian perlu diwujudkan, didokumenkan, dilaksanakan, dipantau dan disemak. Ini bagi memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi seperti mana yang ditetapkan dan konfigurasinya adalah tepat dan tidak berubah tanpa kebenaran.	Pentadbir Sistem ICT KPWKM dan Agensi

BIDANG 08: KESELAMATAN OPERASI

0802 Perisian Berbahaya		
Objektif		
Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.		
080201 Perlindungan dan Kawalan dari Perisian Berbahaya		**Peranan**
	Kawalan terhadap pengesanan, pencegahan dan pemulihan mestilah dilaksanakan untuk melindungi rangkaian dan sistem ICT daripada perisian berbahaya. Perkara-perkara berikut hendaklah dipatuhi: (a) Pengesanan perisian atau program seperti Antivirus, *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS) dan *firewall* mestilah dipasang serta mengikut prosedur penggunaan yang betul dan selamat; (b) Hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa boleh dipasang dan digunakan; (c) Semua perisian atau sistem mestilah diimbas dengan perisian antivirus sebelum digunakan; (d) Semua *antivirus* mesti dikemas kini dengan *pattern antivirus* yang terkini; (e) Kandungan sistem atau maklumat mestilah disemak secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Sesi kesedaran mengenai ancaman baru perisian berbahaya dan cara mengendalikannya hendaklah dihadiri dari semasa ke semasa;	Pentadbir Sistem ICT dan ICTSO

BIDANG 08: KESELAMATAN OPERASI

	(g) Program dan prosedur jaminan kualiti hendaklah diadakan ke atas semua perisian yang dibangunkan; Pengujian jaminan kualiti hendaklah diadakan ke atas semua perisian yang dibangunkan; dan (h) Melaksanakan kajian pematuhan teknikal sistem dari semasa ke semasa.	
080202 Saringan Web		**Peranan**
	Akses kepada laman web luaran yang ditegah oleh KPWKM dan Agensi hendaklah disekat/disaring bagi mengurangkan keterdedahan kepada sebarang bentuk ancaman daripada perisian jahat (*malicious content*) serta sumber laman web yang tidak dibenarkan.	Pentadbir Sistem ICT KPWKM dan Agensi

BIDANG 08: KESELAMATAN OPERASI

0803 Salinan Pendua (*Backup*)		
Objektif		
Memastikan sistem, aplikasi, data, imej dan maklumat mempunyai salinan pendua, berkeupayaan untuk *restore* semula dan melindungi daripada kehilangan maklumat.		
080301 Backup Maklumat		**Peranan**
	Salinan pendua (*backup)* bagi maklumat, perisian dan imej sistem mestilah disimpan dan diuji secara teratur mengikut polisi *backup* yang dipersetujui. Perkara-perkara berikut hendaklah dipatuhi: (a) Penyediaan *backup* ke atas semua sistem perisian dan aplikasi hendaklah dilakukan mengikut jadual *backup* atau setelah mendapat versi terkini; (b) Semua data dan maklumat hendaklah dibuat *backup* mengikut keperluan operasi; (c) Aktiviti pengujian *restore* hendaklah dilaksanakan sekurang-kurangnya sekali setahun bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) Salinan pendua (*backup)* direkod dan disimpan di lokasi yang berlainan dan selamat.	Pentadbir Sistem ICT

BIDANG 08: KESELAMATAN OPERASI

0804 Log dan Pemantauan		
Objektif		
Memastikan log direkodkan dan menjana pembuktian melalui pemantauan.		
080401 Jejak Audit		**Peranan**
	Jejak audit sistem ICT adalah merupakan bukti yang didokumenkan dan adalah merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. (a) Semua rekod aktiviti pengguna, pengecualian, kesilapan dan maklumat keselamatan mestilah dihasilkan, disimpan dan dikaji semula secara berkala; (b) Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan mengikut pekeliling atau peraturan yang sedang berkuat kuasa; dan (c) Catatan jejak audit hendaklah disemak oleh Pentadbir Sistem ICT dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal; (d) Jejak audit juga hendaklah dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan; (e) Jejak audit hendaklah mengandungi maklumat-maklumat berikut: i. Rekod setiap aktiviti transaksi; ii. Identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; iii. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan iv. Maklumat aktiviti sistem yang tidak normal atau	Semua Pengguna dan Pentadbir Sistem ICT

	aktiviti yang tidak mempunyai ciri-ciri keselamatan. (f) Perkara-perkara berikut hendaklah dipatuhi: i. Sistem log hendaklah diwujudkan bagi merekod semua aktiviti harian pengguna dan pentadbiran sistem; ii. Sistem log hendaklah disemak secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan baik pulih dengan segera; iii. Log Audit hendaklah dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; iv. Prosedur untuk memantau penggunaan kemudahan memproses maklumat hendaklah diwujudkan dan hasilnya hendaklah dipantau secara berkala; v. Kemudahan merekod dan maklumat log hendaklah dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; vi. Log kesalahan, kesilapan dan/atau penyalahgunaan hendaklah direkodkan, dianalisis dan diambil tindakan sewajarnya; dan vii. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, pelaporan hendaklah dibuat kepada ICTSO atau CDO.	

BIDANG 08: KESELAMATAN OPERASI

0805 Kawalan Perisian Operasi		
Objektif		
Memastikan integriti sistem operasi.		
080501 Pemasangan Perisian Sistem Operasi		**Peranan**
	Prosedur untuk mengawal pemasangan perisian sistem operasi mestilah dilaksanakan. Perkara-perkara berikut hendaklah dipatuhi: (a) Pengemaskinian perisian operasi, aplikasi dan *program libraries* hanya boleh dilakukan oleh pentadbir terlatih setelah mendapat kelulusan pengurusan; (b) Sistem operasi hanya boleh memiliki "*executable code*" dan tidak boleh memiliki kod pembangunan atau pengkompil; (c) Penggunaan aplikasi dan sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya; (d) Sistem kawalan konfigurasi perlu digunakan untuk mengawal simpanan semua perisian yang dilaksanakan beserta dokumentasi sistem; dan (e) Strategi patah balik kepada sistem asal (*rollback*) perlu disediakan sebelum perubahan dilaksanakan.	Pentadbir Sistem ICT

BIDANG 08: KESELAMATAN OPERASI

0806 Pengurusan Kelemahan Teknikal		
Objektif		
Memastikan kawalan kepada kelemahan teknikal adalah berkesan dan sistematik bagi mengelak serangan perisian berbahaya.		
080601 Kawalan daripada Ancaman Teknikal		**Peranan**
	Maklumat tentang kelemahan teknikal sistem maklumat yang digunakan mestilah diperoleh dengan tepat pada masa yang bersesuaian. Maklumat kelemahan tersebut mestilah dinilai dan langkah bersesuaian hendaklah diambil untuk menangani risiko yang berkaitan. Perkara-perkara berikut hendaklah dipatuhi: (a) Maklumat kelemahan teknikal yang tepat hendaklah diperoleh pada masanya ke atas sistem maklumat yang digunakan; (b) Tahap pendedahan hendaklah dinilai bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT
080602 Kawalan Pemasangan Perisian		**Peranan**
	Kawalan kepada pemasangan perisian oleh pengguna mestilah diwujudkan dan dilaksanakan secara berkesan; dan Hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa boleh dipasang dan digunakan.	Semua Pengguna

BIDANG 08: KESELAMATAN OPERASI

080603 Perisikan Ancaman		Peranan
	Maklumat berkaitan ancaman keselamatan hendaklah dikumpul dan dianalisis bagi memudahkan tindakan pencegahan diambil serta mengurangkan kesan ancaman terhadap organisasi. Laporan berkaitan perisikan ancaman keselamatan hendaklah dikongsi dengan pihak yang berkenaan bagi memastikan tindakan mitigasi yang sesuai boleh dilaksanakan. Program kesedaran hendaklah dilaksanakan dengan mengambil kira laporan dan analisa daripada perisikan ancaman.	Semua Pengguna

BIDANG 08: KESELAMATAN OPERASI

0807 Pertimbangan Audit Sistem Maklumat		
Objektif		
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan dilaksanakan.		
080701 Kawalan Audit Sistem Maklumat		**Peranan**
	Keperluan audit dan aktiviti-aktiviti yang melibatkan pengesahan sistem operasi mestilah dirancang dengan teliti dan dipersetujui untuk mengurangkan gangguan kepada perkhidmatan. Perkara-perkara berikut hendaklah dipatuhi: (a) Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat; (b) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi hendaklah dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; dan (c) Capaian ke atas peralatan audit sistem maklumat hendaklah dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO & Audit Dalam

BIDANG 09: PENGURUSAN KOMUNIKASI

0901 Pengurusan Keselamatan Rangkaian		
Objektif		
Memastikan perlindungan maklumat dalam rangkaian dan kemudahan sokongan pemprosesan maklumat dalam rangkaian.		
090101 Keselamatan Rangkaian		**Peranan**
	Infrastruktur Rangkaian mestilah dikawal dan diurus sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Perkara-perkara berikut hendaklah dipatuhi: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas daripada risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian ICT; (f) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan KPWKM dan Agensi; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;	Pentadbir Rangkaian ICT dan ICTSO

BIDANG 09: PENGURUSAN KOMUNIKASI

	(h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan menceroboh dan aktiviti- aktiviti lain yang boleh mengancam sistem dan maklumat KPWKM dan Agensi; (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian adalah di bawah kawalan KPWKM dan Agensi; (k) Kakitangan KPWKM dan Agensi hanya dibenarkan menggunakan rangkaian KPWKM dan Agensi sahaja dan penggunaan *modem* atau *mobile broadband* adalah tertakluk kepada peraturan semasa KPWKM dan Agensi; dan (l) Kemudahan bagi rangkaian tanpa wayar hendaklah dipastikan kawalan keselamatan.	
090102 Keselamatan Perkhidmatan Rangkaian		**Peranan**
	Pengurusan bagi semua perkhidmatan rangkaian (*inhouse atau outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenalpasti dan dimasukkan dalam perjanjian perkhidmatan rangkaian.	Pentadbir Rangkaian dan ICTSO
090103 Pengasingan Rangkaian		**Peranan**
	Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian KPWKM dan Agensi.	Pentadbir Rangkaian dan ICTSO

BIDANG 09: PENGURUSAN KOMUNIKASI

0902 Pemindahan Maklumat		
Objektif		
Memastikan keselamatan perpindahan/pertukaran maklumat dan perisian antara KPWKM dan Agensi dengan pihak luar terjamin.		
090201 Dasar dan Prosedur Pemindahan Maklumat		**Peranan**
	Perkara-perkara seperti berikut hendaklah dipatuhi: (a) Dasar, prosedur dan kawalan pemindahan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Terma pemindahan maklumat dan perisian di antara KPWKM dan Agensi dengan pihak luar hendaklah dimasukkan dalam Perjanjian; (c) Media yang mengandungi maklumat hendaklah dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan maklumat; dan (d) Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya.	Pengguna, Pentadbir Rangkaian, Pentadbir Emel, Pentadbir Sistem Aplikasi, Pemilik Sistem dan ICTSO

BIDANG 09: PENGURUSAN KOMUNIKASI

090202 Perjanjian Mengenai Pemindahan Maklumat		**Peranan**
	KPWKM dan Agensi hendaklah mengambil kira keselamatan maklumat organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara KPWKM dan Agensi dengan pihak luar. Perkara-perkara berikut hendaklah dipertimbangkan: KPWKM dan Agensi hendaklah mengambil kira keselamatan maklumat organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara KPWKM dan Agensi dengan pihak luar. Perkara-perkara berikut hendaklah dipertimbangkan: (a) Tanggungjawab pengurusan bagi mengawal penghantaran dan penerimaan maklumat organisasi; (b) Prosedur bagi pengesanan maklumat organisasi semasa pemindahan maklumat; dan (c) Tanggungjawab dan liabiliti sekiranya berlaku insiden keselamatan siber seperti kehilangan data.	CDO dan Pengurus ICT ICTSO

BIDANG 09: PENGURUSAN KOMUNIKASI

090203 Pengurusan mel Elektronik (E-mel)		Peranan
	Penggunaan mel elektronik (e-mel) di KPWKM dan Agensi hendaklah dipantau secara berterusan oleh Pentadbir Sistem e-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam peraturan-peraturan yang sedang berkuat kuasa Penggunaan mel elektronik (e-mel) di KPWKM dan Agensi hendaklah dipantau secara berterusan oleh Pentadbir Sistem e-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam peraturan-peraturan yang sedang berkuat kuasa. Perkara-perkara seperti berikut hendaklah dipatuhi: (a) Hanya e-mel rasmi yang boleh digunakan untuk urusan rasmi; (b) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (c) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh KPWKM dan Agensi (d) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; (e) Pengguna hendaklah mengelak daripada membuka e-mel daripada penghantar yang tidak diketahui atau diragui; (f) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pihak yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; (g) E-mel yang tidak mempunyai nilai arkib, hendaklah diambil tindakan dan sekiranya e-mel tersebut tidak diperlukan lagi boleh dihapuskan;	Pengguna, Pentadbir Emel, ICTSO

	(i) Pemilik e-mel hendaklah memastikan tarikh dan masa sistem komputer adalah tepat bagi memastikan kesahihan masa penghantaran dan penerimaan; (j) E-mel persendirian (seperti yahoo.com, gmail.com, dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan (k) Kakitangan KPWKM dan Agensi hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing- masing.	
090204 Kerahsiaan dan *Non-Disclosure Agreement*		**Peranan**
	Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* hendaklah mengambil kira keperluan organisasi dan hendaklah disemak dan didokumentasikan dari semasa ke semasa.	CDO, ICTSO

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

1001 Keperluan Keselamatan Sistem Maklumat		
Objektif		
Memastikan keselamatan maklumat adalah merupakan sebahagian daripada proses pembangunan sistem. Ini merangkumi keselamatan maklumat apabila menggunakan rangkaian luar.		
100101 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat		**Peranan**
	Keperluan keselamatan maklumat bagi pembangunan sistem baru dan penambahbaikan hendaklah mematuhi perkara-perkara berikut: (a) Semua sistem yang dibangunkan sama ada secara dalaman (*in house*) atau (*outsource*) hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber KPWKM dan Agensi; (b) Penyediaan rekabentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan (c) Ujian keselamatan hendaklah dilakukan di setiap peringkat pembangunan sistem bagi memastikan kesahihan dan integriti data.	Pemilik dan Pentadbir Sistem
100102 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum		**Peranan**
	Keperluan insuran perlu untuk melindungi kepentingan KPWKM dan Agensi. Maklumat aplikasi yang melalui rangkaian umum (*public networks*) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara- perkara berikut hendaklah dipatuhi: (a) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*);	Pentadbir Sistem dan ICTSO

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

	(b) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; (c) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan perkhidmatan ICT; (d) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak; (e) Liabiliti yang berkaitan dengan mana-mana kes transaksi fraud; dan (f) Keperluan insuran perlu untuk melindungi kepentingan KPWKM dan Agensi.	
100103 Melindungi Perkhidmatan Transaksi Aplikasi		**Peranan**
	Keperluan insuran perlu untuk melindungi kepentingan KPWKM dan Agensi. Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej. Perkara-perkara berikut hendaklah dipertimbangkan: (a) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; (b) Memastikan semua aspek transaksi dipatuhi; (c) Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; (d) Mengekalkan kerahsiaan maklumat; (e) Mengekalkan privasi pihak yang terlibat; (f) Komunikasi antara semua pihak yang terlibat dirahsiakan; dan (g) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. (h) Pihak yang mengeluar dan mengekalkan pensijilan digital atau tandatangan adalah dilantik oleh	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

	Kerajaan.	

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

100104 Menyembunyikan Data (*Data Masking*)		**Peranan**
	Sistem aplikasi yang mewujudkan, memproses, menyimpan, menghantar dan meluluskan maklumat sensitif (contoh no. kad pengenalan, PII) hendaklah diberikan penyulitan atau kaedah menyembunyikan data bagi mengehadkan pendedahan data sensitif termasuk maklumat yang boleh dikenal pasti secara peribadi dan untuk mematuhi keperluan undang-undang, berkanun, peraturan dan kontrak.	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem
1002 Keselamatan Dalam Pembangunan dan Sokongan Sistem		
Objektif		
Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.		
100201 Polisi Keselamatan Dalam Pembangunan Sistem		**Peranan**
	Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan untuk perkembangan dalam organisasi. Perkara- perkara berikut hendaklah dipertimbangkan: (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 *repository*; (f) Keselamatan dalam kawalan versi; (g) Keperluan pengetahuan keselamatan dalam pembangunan perisian; dan (h) Bagi pembangunan secara penyumberluaran	Pentadbir Sistem dan ICTSO

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

	(*outscource*), pembekal yang dilantik berkebolehan untuk mengenalpasti dan menambah baik kelemahan dalam pembangunan sistem.	
100202 Prosedur Kawalan Perubahan Sistem		**Peranan**
	Perubahan ke atas sistem hendaklah dikawal. Perkara-perkara berikut hendaklah dipatuhi: (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 hendaklah dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan KPWKM dan Agensi (c) Pentadbir sistem hendaklah bertanggungjawab untuk memantau penambahbaikan dan perubahan yang dilakukan oleh pembekal; dan (d) Kawalan hendaklah dibuat ke atas sebarang perubahan atau pindaan ke atas sistem bagi memastikan ianya terhad mengikut keperluan sahaja.	Pentadbir Sistem dan ICTSO

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

100203 Kajian Teknikal Selepas Permohonan Perubahan Platform		Peranan
	Perkara-perkara berikut hendaklah dipatuhi: (a) Kawalan aplikasi dan prosedur integriti disemak untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; (b) Perubahan platform dimaklumkan dari semasa ke semasa bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan (c) Memastikan perubahan yang sesuai dibuat kepada pelan kesinambungan organisasi.	Pentadbir Sistem Aplikasi dan ICTSO

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

100204 Sekatan Perubahan Pakej Perisian (*Software Packages*)		**Peranan**
	Perubahan kepada pakej perisian adalah tidak digalakkan tetapi terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem Aplikasi dan ICTSO
100205 Prinsip Kejuruteraan Keselamatan Sistem (*Secure System Engineering Principles*)		**Peranan**
	(a) Prinsip-prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumentasi, diselenggara dan diguna pakai dalam pelaksanaan sistem. (b) Keselamatan hendaklah diambil kira dalam semua peringkat pembangunan sistem. (c) Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa bagi memastikan keberkesanan kepada (d) keselamatan maklumat.	Pentadbir Sistem Aplikasi dan ICTSO
100206 Keselamatan Persekitaran Pembangunan Sistem		**Peranan**
	Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem (*development lifecycle*).	Pentadbir Sistem, Pengurus ICT

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

100207 Pembangunan Sistem Secara *Outsource*		**Peranan**
	(a) Aktiviti pembangunan sistem yang dijalankan oleh khidmat luaran hendaklah diselia dan dipantau. Perkara-perkara berikut hendaklah dipatuhi: (b) Pembangunan perisian secara outsource hendaklah diselia dan dipantau oleh pemilik sistem/pentadbir sistem; (c) Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik Kerajaan; (d) Kod sumber (*source code*) yang diserahkan kepada Kerajaan mesti bebas daripada sebarang ralat; dan (e) Maklumat, prosedur, dan dokumen yang digunakan semasa pembangunan secara *outsource* adalah menjadi rahsia Kerajaan yang tidak boleh disebar dan didedahkan.	Pemilik Sistem dan Pentadbir Sistem

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

100208 Pengujian Keselamatan Sistem		**Peranan**
	Pengujian fungsian keselamatan sistem hendaklah dilaksanakan bagi memastikan penentusahan semasa proses pembangunan. Perkara-perkara berikut hendaklah dipatuhi: (a) Pengujian keselamatan sistem hendaklah dijalankan semasa pembangunan; (b) Sistem baru dan penambahbaikan sistem yang dikategorikan kritikal hendaklah menjalani ujian *Security Posture Assessment* (SPA) termasuk penyediaan jadual terperinci aktiviti, ujian input dan output (*input* and *output validation*); (c) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; (d) Mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi; (e) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti sebarang pencerobohan maklumat sama ada kerana kesilapan atau disengajakan; dan (f) Menjalankan proses semak ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan dan kesesuaian.	Pentadbir Sistem dan ICTSO
100209 Pengujian Penerimaan Sistem		**Peranan**
	Pengujian penerimaan semua sistem baru dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai. Pengujian fungsian keselamatan sistem hendaklah dilaksanakan bagi memastikan penentusahan semasa proses pembangunan.	Pentadbir Sistem dan ICTSO

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

100210 Pengekodan Selamat (*Secure Coding*)		**Peranan**
	Prinsip pengekodan selamat hendaklah diwujudkan, dikemaskini dan pelaksanaannya diuji pada sistem aplikasi bagi mengurangkan risiko kelemahan sistem aplikasi yang dibangunkan. Pengekodan selamat hendaklah mengikut amalan terbaik yang terdapat di dalam industri pengaturcaraan komputer.	

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

1003 Data Ujian		
Objektif		
Memastikan keselamatan data yang digunakan untuk pengujian.		
100301 Perlindungan Data Ujian		**Peranan**
	Data ujian hendaklah dipilih dengan berhati-hati, dilindungi dan dikawal daripada sebarang kebocoran maklumat. Perkara-perkara berikut hendaklah dipatuhi: (a) Penggunaan data operasi yang mengandungi maklumat peribadi atau sebarang maklumat sulit harus dielakkan. Sekiranya penggunaan tidak dapat dielakkan, maklumat tersebut hendaklah dilindungi dengan cara pembuangan atau pengubahsuaian serta perlu mendapat kelulusan. (b) Memastikan kawalan akses dilaksanakan; (c) Data ujian perlu dipadam daripada persekitaran pengujian selepas selesai ujian dijalankan; (d) Penyalinan dan penggunaan data operasi; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem dan Pentadbir Sistem

BIDANG 11:-HUBUNGAN DENGAN PEMBEKAL

1101 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal		
Objektif		
Memastikan perlindungan pada aset KPWKM dan Agensi yang boleh diakses oleh pembekal.		
110101 Polisi Keselamatan Maklumat Untuk Pembekal		**Peranan**
	Keperluan keselamatan maklumat hendaklah dipatuhi oleh pembekal dan didokumentasi bagi mengurangkan risiko kepada aset KPWKM dan Agensi yang boleh diakses oleh pembekal. Perkara-perkara berikut hendaklah dipatuhi: (a) Mengenal pasti jenis pembekal yang dibenarkan mengakses maklumat organisasi; (b) Pengurusan pembekal adalah tertakluk kepada peraturan yang sedang berkuat kuasa; (c) Mengawal dan memantau akses pembekal; (d) Keperluan minimum keselamatan maklumat bagi setiap pembekal seperti keperluan perundangan atau pekeliling berkaitan hendaklah dinyatakan dalam perjanjian; dan (e) Memastikan pembekal diberikan taklimat keselamatan dan menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber KPWKM, Agensi dan Pihak Ketiga/Kontraktor seperti di **Lampiran 1**.	ICTSO, Pemilik Sistem, Pembekal, Pihak Ketiga

BIDANG 11:-HUBUNGAN DENGAN PEMBEKAL

110102 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal		**Peranan**
	Semua keperluan keselamatan maklumat untuk mengurangkan risiko kepada aset serta maklumat KPWKM dan Agensi hendaklah didokumenkan di dalam kontrak perjanjian dan hendaklah dipersetujui oleh setiap Pembekal yang boleh mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur bagi pengurusan maklumat KPWKM dan Agensi. Pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak KPWKM dan Agensi selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.	Pemilik Sistem dan ICTSO

BIDANG 11:-HUBUNGAN DENGAN PEMBEKAL

	Perkara-perkara berikut hendaklah dipatuhi: (a) KPWKM dan Agensi hendaklah memilih syarikat pembekal yang 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 pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; (d) Produk atau perkhidmatan yang ditawarkan oleh 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 pembekal; (f) Laporan penilaian pihak ketiga yang dikemukakan oleh 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; dan v. Andaian yang dibuat berkaitan dengan skop penilaian. (g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan KPWKM dan Agensi; (h) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh KPWKM dan	ICTSO dan Pemilik Sistem

BIDANG 11:-HUBUNGAN DENGAN PEMBEKAL

	Agensi (i) Kewajipan pembekal mematuhi keperluan keselamatan maklumat.	
110103 Kawalan Rantaian Bekalan Teknologi Maklumat dan Komunikasi		**Peranan**
	Perjanjian dengan pembekal hendaklah mengambil kira keperluan bagi menangani risiko keselamatan maklumat yang berkaitan dengan rantaian bekalan perkhidmatan dan produk bagi teknologi maklumat dan komunikasi. Perkara-perkara berikut hendaklah dipatuhi: (a) Penentuan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada sub kontraktor bagi perkhidmatan; (c) Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada pembekal-pembekal lain bagi pembekalan produk; (d) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; (e) Komponen produk dan perkhidmatan kritikal serta komponen tambahan hendaklah dikenal pasti; (f) Pembekal hendaklah memberi jaminan bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; dan (g) Kaedah-kaedah perkongsian maklumat dalam rantaian bekalan (*supply chain*) antara KPWKM dan Agensi dan pembekal hendaklah ditentukan.	Pemilik Sistem dan ICTSO

BIDANG 11:-HUBUNGAN DENGAN PEMBEKAL

1102 Pengurusan Penyampaian Perkhidmatan Pembekal		
Objektif		
KPWKM dan Agensi hendaklah sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal.		
110201 Pemantauan dan Kajian Perkhidmatan Pembekal		**Peranan**
	KPWKM dan Agensi hendaklah sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal. Perkara-perkara berikut hendaklah dipatuhi: (a) Pemantauan tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan; (b) Mengkaji semula laporan perkhidmatan yang disediakan oleh pembekal dan mengemukakan status kemajuan; dan (c) Memaklumkan insiden keselamatan siber kepada pembekal untuk tindakan sebagaimana yang ditetapkan dalam perjanjian.	ICTSO dan Pemilik Sistem
110202 Pengurusan Perubahan Pada Perkhidmatan Pembekal		**Peranan**
	Perubahan kepada peruntukan perkhidmatan oleh Pembekal yang disebabkan oleh perubahan pada Polisi Keselamatan Siber KPWKM, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan data dan maklumat, sistem penyampaian dan proses perkhidmatan yang terlibat dan risiko yang berkaitan. Perkara-perkara berikut hendaklah dipatuhi: (a) Memastikan perubahan dalam perkhidmatan pembekal	Pemilik Sistem dan ICTSO

	dipersetujui bersama dan menguntungkan bagi pihak KPWKM dan Agensi; (b) Memastikan perubahan dalam perjanjian dengan pembekal mengambil kira maklumat kritikal KPWKM dan Agensi, sistem, proses serta penilaian risiko terlibat; (c) Perubahan yang dilakukan oleh KPWKM dan Agensi untuk meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; (d) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	

BIDANG 11:-HUBUNGAN DENGAN PEMBEKAL

1103 Keselamatan Maklumat dan Pengurusan Penyampaian Perkhidmatan Pengkomputeran Awan (*Cloud*) oleh Pembekal		
Objektif		
Memastikan keselamatan maklumat dan sistem yang diletakkan di dalam persekitaran awan dari aspek kerahsiaan, integriti serta ketersediaan melalui pelaksanaan langkah keselamatan yang komprehensif serta mematuhi peraturan dan undang-undang sedia ada.		
110301 Pengurusan Pengkomputeran Awan		**Peranan**
	KPWKM dan Agensi hendaklah memastikan keselamatan maklumat kerajaan adalah terjamin sebelum, semasa dan selepas penggunaan perkhidmatan pengkomputeran awan dengan mengambil kira perkara di bawah: (a) Memastikan bahawa penilaian risiko dilaksanakan sebelum dan semasa menggunakan perkhidmatan pengkomputeran awan; (b) Mendokumentasikan dengan jelas tanggungjawab dan peranan pembekal perkhidmatan pengkomputeran awan serta KPWKM dan Agensi; dan (c) Memastikan perjanjian yang jelas di antara pembekal perkhidmatan pengkomputeran awan serta KPWKM dan Agensi. Perjanjian tersebut hendaklah mengandungi perkara di bawah: i. Pembekal hendaklah mempunyai pensijilan keselamatan yang berkaitan; ii. Pembekal hendaklah menyediakan mekanisme kawalan akses yang memenuhi keperluan KPWKM dan Agensi; dan iii. Pembekal hendaklah menyediakan perisian bagi melindungi keselamatan maklumat daripada perisian hasad.	Pemilik Sistem dan ICTSO

BIDANG 12:-PENGURUSAN INSIDEN KESELAMATAN SIBER

1201 Pengurusan dan Penambahbaikan Insiden Keselamatan Siber		
Objektif		
Memastikan insiden keselamatan siber siber dikendalikan dengan cepat, teratur dan berkesan bagi meminimumkan kesan insiden keselamatan siber dan mengenalpasti komunikasi serta kelemahan apabila berlaku insiden keselamatan siber.		
120101 Tanggungjawab dan Prosedur		**Peranan**
	Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan siber.	CDO, ICTSO, CSIRT KPWKM dan Agensi
120102 Mekanisme Pelaporan Insiden Keselamatan Siber		**Peranan**
	Insiden keselamatan siber bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar polisi keselamatan siber sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan siber seperti berikut hendaklah dilaporkan kepada ICTSO KPWKM dan Agensi, CDO KPWKM dan Agensi, CSIRT KPWKM dan Agensi dan juga NACSA dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak yang tidak diberi kuasa atau, disyaki hilang; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi	Pemilik Sistem dan ICTSO

	tersalah hantar; (e) Berlaku percubaan menceroboh, penyelewengan ICT berdasarkan pekeliling yang berkuat kuasa; dan (f) Prosedur pelaporan insiden keselamatan siber berdasarkan pekeliling yang berkuat kuasa.	

BIDANG 12:-PENGURUSAN INSIDEN KESELAMATAN SIBER

120103 Melaporkan Kelemahan Keselamatan Siber		**Peranan**
	Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat KPWKM dan Agensi dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT kepada ICTSO KPWKM dan Agensi atau CSIRT KPWKM dan Agensi.	Semua Pengguna
120104 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Siber		**Peranan**
	Menentukan keutamaan tindakan ke atas insiden keselamatan siber. Tindakan ke atas insiden keselamatan siber hendaklah dilaporkan berasaskan tahap kritikal sesuatu insiden keselamatan siber mengikut keutamaan 1 dan keutamaan 2.	ICTSO, CSIRT KPWKM dan Agensi
120105 Pengendalian Insiden Keselamatan Siber		**Peranan**
	Insiden keselamatan siber hendaklah dikendalikan mengikut prosedur yang telah ditetapkan. Kawalan-kawalan berikut hendaklah diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden keselamatan siber: (a) Mengumpul bukti secepat mungkin selepas insiden keselamatan siber berlaku; (b) Menjalankan kajian forensik sekiranya perlu; (c) Menghubungi pihak yang berkenaan dengan segera; (d) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (f) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; (g) Menyediakan tindakan pemulihan segera; (h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu; dan (i) KPWKM dan Agensi hendaklah menentukan prosedur untuk mengenal pasti koleksi, kaedah pemerolehan	ICTSO, CSIRT KPWKM dan Agensi

	dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti.	

BIDANG 12:-PENGURUSAN INSIDEN KESELAMATAN SIBER

120106 Pembelajaran daripada Insiden Keselamatan Siber		**Peranan**
	Organisasi perlu mewujudkan mekanisme untuk mengumpul, mengukur, dan memantau maklumat tentang jenis insiden keselamatan siber, jumlah, dan kos bagi mengurangkan kemungkinan atau akibat insiden keselamatan siber pada masa hadapan. Maklumat yang diperoleh daripada penilaian kejadian insiden keselamatan siber harus digunakan untuk: a) Menambah baik pelan pengurusan insiden keselamatan siber termasuk senario dan prosedur kejadian; b) Mengenal pasti kejadian berulang atau serius dan penyebabnya untuk mengemas kini penilaian risiko keselamatan siber organisasi dan menentukan serta melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan kemungkinan atau akibat kejadian insiden keselamatan siber yang sama pada masa hadapan; dan c) Meningkatkan kesedaran serta latihan pengguna dengan memberikan contoh serta kaedah menanganinya dan kaedah menghindarinya pada masa hadapan.	ICTSO dan CSIRT KPWKM dan Agensi

BIDANG 13:-ASPEK KESELAMATAN MAKLUMAT DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1301 Pelan Kesinambungan Perkhidmatan		
Objektif		
Keselamatan maklumat hendaklah dimasukkan ke dalam sistem pengurusan kesinambungan perkhidmatan.		
130101 Rancangan Keselamatan Maklumat dalam Pelan Kesinambungan Perkhidmatan		**Peranan**
	Pihak KPWKM dan Agensi hendaklah memastikan Pelan Kesinambungan Perkhidmatan dibangunkan bagi menentukan pendekatan yang menyeluruh diambil bagi memastikan kesinambungan perkhidmatan KPWKM dan Agensi. Ini adalah bertujuan untuk memastikan ketersediaan perkhidmatan KPWKM dan Agensi tidak terganggu selain dapat mengenal pasti aspek keselamatan maklumat dalam pelan Pengurusan Kesinambungan Perkhidmatan (PKP).	CDO, ICTSO dan DRT
130102 Mekanisme Pelaporan Insiden Keselamatan Maklumat		**Peranan**
	Pihak KPWKM dan Agensi hendaklah memastikan aspek keselamatan maklumat dalam pelan Pengurusan Kesinambungan Perkhidmatan (PKP) diwujudkan, didokumentasi, dilaksana dan dikemas kini (proses, prosedur serta kawalan) untuk memastikan tahap keselamatan maklumat dalam kesinambungan perkhidmatan menepati keperluan semasa berlaku gangguan/bencana. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Jawatankuasa Pemandu PKP.	CDO, ICTSO dan DRT

BIDANG 13:-ASPEK KESELAMATAN MAKLUMAT DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

	Perkara-perkara berikut hendaklah dipatuhi: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan; (b) Mengenal pasti insiden keselamatan siber atau ancaman yang boleh mengakibatkan gangguan terhadap perkhidmatan KPWKM dan Agensi serta kemungkinan dan impak gangguan tersebut terhadap keselamatan ICT; (c) Menjalankan analisis impak perkhidmatan; (d) Melaksanakan simulasi terhadap prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (e) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (f) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (g) Membuat *backup* mengikut prosedur yang telah ditetapkan; dan (h) Menguji, menyelenggara dan mengemaskini pelan PKP sekurang- kurangnya setahun sekali. Pelan PKP hendaklah dibangunkan, didokumentasikan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel utama KPWKM dan Agensi, pembekal dan pihak ketiga beserta nombor yang boleh dihubungi (faksimili, telefon, sistem pesanan ringkas, dan e-mel). Senarai personel kedua juga hendaklah disediakan sebagai menggantikan personel utama yang tidak dapat hadir untuk menangani insiden keselamatan siber;	CIO, ICTSO dan DRT

BIDANG 13:-ASPEK KESELAMATAN MAKLUMAT DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

	(c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal dan pihak ketiga untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Salinan dokumentasi pelan PKP hendaklah disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan PKP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi perkhidmatan untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. KPWKM dan Agensi hendaklah memastikan salinan dokumentasi pelan PKP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	
130103 Mengesah, Mengkaji semula dan Menilai Keselamatan Maklumat dalam Pelan Pengurusan Kesinambungan Perkhidmatan		**Peranan**
	KPWKM dan Agensi hendaklah mengesahkan kawalan terhadap keselamatan maklumat dalam pelan Pengurusan Kesinambungan Perkhidmatan (PKP). Semakan PKP dibuat setiap dua (2) tahun sekali atau sekiranya terdapat perubahan untuk memastikan pelan berkenaan sahih dan berkesan semasa berlaku gangguan/ bencana.	

BIDANG 13:-ASPEK KESELAMATAN MAKLUMAT DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1302 Kesinambungan Perkhidmatan ICT		
Objektif		
Keselamatan maklumat hendaklah dimasukkan ke dalam sistem pengurusan kesinambungan perkhidmatan.		
130201 Ketersediaan ICT untuk Kesinambungan Operasi		**Peranan**
	Prosedur DRMP (Pelan Pengurusan Pemulihan Bencana) dan DRTP (Pelan Teknikal Pemulihan Bencana) hendaklah disediakan, didokumenkan, dilaksanakan dan diselenggara bagi menjamin kesinambungan perkhidmatan ketika berlaku insiden keselamatan siber. Perkara yang perlu dilaksanakan adalah seperti yang berikut: (a) Mengemas kini DRMP dan DRTP jika berlaku perubahan kepada fungsi kritikal KPWKM dan agensi; (b) Mengemas kini struktur tadbir urus DRMP dan DRTP KPWKM dan agensi; (c) Melaksanakan pengujian DRMP dan DRTP secara berkala atau apabila berlaku perubahan kepada peraturan yang sedang berkuat kuasa untuk memastikan pelan berkenaan sahih dan berkesan semasa berlaku gangguan/bencana; (d) Melaksanakan post-mortem dan mengemaskini DRMP dan DRTP; dan (e) Memastikan pasukan DRMP dan DRTP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksanakan DRMP dan DRTP.	Pengurus ICT

BIDANG 13:-ASPEK KESELAMATAN MAKLUMAT DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1303 *Redundancies*		
Objektif		
Memastikan ketersediaan kemudahan pemprosesan maklumat.		
130301 Ketersediaan Kemudahan Pemprosesan Maklumat		**Peranan**
	Kemudahan pemprosesan maklumat hendaklah mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan maklumat.	Pengurus ICT

BIDANG 14-PEMATUHAN

1401 Pematuhan Terhadap Keperluan Perundangan dan Perjanjian Kontrak		
Objektif		
Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak daripada pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.		
140101 Mengenal pasti Undang-Undang dan Perjanjian Kontrak		**Peranan**
	Semua dokumen perundangan seperti undang-undang berkanun, peraturan dan keperluan kontrak yang berkaitan dengan Kementerian dan Agensi hendaklah ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat. Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga di KPWKM dan Agensi adalah seperti di **Lampiran 4.**	Semua Pengguna

BIDANG 14-PEMATUHAN

140102 Hak Harta Intelek (*Intellectual Property Rights* – IPR)		**Peranan**
	Prosedur-prosedur yang sesuai akan dilaksanakan untuk memastikan keselarasan dengan perundangan, peraturan dan juga keperluan kontrak yang berkaitan dengan IPR dan juga perlesenan perisian. KPWKM dan Agensi akan mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. Perkara-perkara berikut hendaklah dipatuhi: (a) Pematuhan terhadap hak cipta yang berkaitan dengan perisian proprietari,dan reka bentuk yang diperoleh daripada KPWKM dan Agensi; (b) Pematuhan terhadap perlesenan menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperoleh daripada KPWKM dan Agensi; (c) KPWKM dan Agensi hendaklah memastikan pematuhan terhadap hakcipta produk dan keperluan pelesenan; dan (d) Perisian atau sistem maklumat yang dibangunkan oleh KPWKM dan Agensi adalah menjadi harta intelek KPWKM dan Agensi.	Semua Pengguna

BIDANG 14-PEMATUHAN

140103 Perlindungan Rekod		**Peranan**
	Rekod-rekod yang penting (fizikal atau media) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, pelepasan yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak, dan keperluan KPWKM dan Agensi. Perkara-perkara berikut hendaklah dipertimbangkan: (a) Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat (Rujuk Dasar Pengurusan Rekod dan Arkib Elektronik 2003); (b) Jadual pelupusan dan penyimpanan rekod hendaklah dikenal pasti; dan (c) Inventori rekod dikemaskini.	Semua Pengguna
140104 Privasi dan Perlindungan Maklumat Peribadi		**Peranan**
	KPWKM dan Agensi hendaklah mengenal pasti privasi dan perlindungan maklumat peribadi pengguna dijamin seperti yang tertakluk dalam undang-undang Kerajaan Malaysia dan peraturan-peraturan yang berkenaan.	Semua Pengguna

BIDANG 14-PEMATUHAN

140105 Kawalan Kriptografi		Peranan
	Semua dokumen perundangan seperti undang-undang berkanun, peraturan dan keperluan kontrak yang berkaitan dengan Kementerian dan Agensi hendaklah ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat. Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga di KPWKM dan Agensi adalah seperti di **Lampiran 4**. Kawalan kriptografi hendaklah diguna pakai dengan mematuhi semua perjanjian, undang-undang, dan peraturan-peraturan yang berkaitan. Perkara-perkara berikut hendaklah dipatuhi: (a) Kawalan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi-fungsi kriptografi; (b) Kawalan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah/direka untuk mempunyai fungsi kriptografi; (c) Kawalan ke atas penggunaan enkripsi; dan (d) Kaedah akses oleh pihak berkuasa Malaysia bagi maklumat enkripsi perkakasan dan perisian.	Semua Pengguna

BIDANG 14-PEMATUHAN

1402 Kajian Keselamatan Maklumat		
Objektif		
Memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur KPWKM dan Agensi.		
140201 Kajian Semula Keselamatan Maklumat oleh Pihak Berkecuali		**Peranan**
	Kajian Semula Keselamatan Maklumat oleh pihak berkecuali Penilaian keselamatan maklumat oleh pihak berkecuali hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur seperti berikut: (a) undang-undang dan peraturan yang memberi kesan kepada perubahan organisasi; (b) insiden keselamatan siber yang berlaku; (c) organisasi memulakan perkhidmatan baharu atau mengubah perkhidmatan semasa; atau (d) organisasi mengubah kawalan dan prosedur keselamatan maklumat dengan ketara.	CDO, ICTSO
140202 Pematuhan Dasar dan Standard / Piawaian		**Peranan**
	Kajian teknikal hendaklah dilakukan setahun sekali atau mengikut keperluan. Sekiranya kajian semula mengenal pasti ketidakpatuhan, KPWKM dan Agensi hendaklah: (a) Mengenal pasti punca-punca ketidakpatuhan; (b) Menilai keperluan tindakan untuk mencapai pematuhan tindakan pembetulan hendaklah dilaksanakan; dan (c) Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanan serta mengenal pasti kelemahan dan kekurangannya.	CDO, ICTSO

BIDANG 14-PEMATUHAN

140203 Pematuhan Kajian Teknikal		**Peranan**
	Sistem maklumat hendaklah sentiasa dikaji supaya selaras dengan pematuhan dasar dan standard keselamatan maklumat KPWKM dan Agensi (seperti *Security Posture Assessment* – SPA). Kajian teknikal hendaklah dilakukan setahun sekali atau mengikut kesesuaian.	Pengurus ICT

GLOSARI

Ancaman	Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CD ROM, thumb drive untuk sebarang kemungkinan adanya virus.
Aset ICT	Bermaksud semua yang mempunyai nilai kepada KPWKM dan Agensi merangkumi 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.
CSIRT	Computer Security Incident Response Team atau Pasukan Tindak Balas Insiden Keselamatan Siber KPWKM dan Agensi. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan siber di agensi masing-masing dan agensi di bawah kawalannya.
CDO	Chief Digital Officer Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Clear Desk	Tidak meninggalkan sebarang dokumen yang sensitif di atas meja.
Clear Screen	Tidak memaparkan sebarang maklumat sensitif apabila komputer berkenaan ditinggalkan.
Denial of service	Halangan pemberian perkhidmatan.

Downloading	Aktiviti muat turun sesuatu perisian.
DRT	Disaster Recovery Team (Pasukan Pemulihan Bencana)
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah. Teks biasa (plaintext) akan ditukar kepada kod yang tidak difahami dan kod yang tidak difahami ini akan menjadi versi teks cipher. Bagi mendapatkan semula teks biasa tersebut, proses penyahsulitan digunakan.
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).
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi).
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.

Internet	Sistem rangkaian seluruh dunia, dimana 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.
ISM	Institut Sosial Malaysia
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.
Insiden Keselamatan Siber	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat.
JKM	Jabatan Kebajikan Masyarakat
JPICT	Jawatankuasa Pemandu ICT KPWKM
JKICT	Jawatankuasa Keselamatan ICT KPWKM
JPW	Jabatan Pembangunan Wanita

Kriptografi	Satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Log-out	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
LPPKN	Lembaga Penduduk dan Pembangunan Negara
TAGS	Tribunal bagi Antigangguan Seksual

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.
Mobile Code	Kod perisian yang dipindahkan dari satu komputer ke komputer lain dan melaksanakan secara automatik fungsi–fungsi tertentu dengan sedikit atau tanpa interaksi daripada pengguna.
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.
Penilaian Risiko	Penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
Perisian Aplikasi	Ia merujuk kepada perisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau KPWKM dan Agensi.
Public-Key Infrastructure (PKI)	Prasarana Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Risiko	Kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.
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.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya segmentasi rangkaian boleh dilaksanakan. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan pelanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible PowerSupply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada 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.
Vulnerability (Kerentanan)	Sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER KPWKM, AGENSI & PIHAK KETIGA / KONTRAKTOR KPWKM

KEMENTERIAN PEMBANGUNAN WANITA,
KELUARGA DAN MASYARAKAT

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
OLEH PIHAK KETIGA/KONTRAKTOR
KEMENTERIAN PEMBANGUNAN WANITA, KELUARGA DAN MASYARAKAT

Nama Syarikat :
Wakil Syarikat :
No Kad Pengenalan :
Jawatan :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....
(Tandatangan Pihak Ketiga/ Kontraktor

Tarikh

Pengesahan Pegawai Keselamatan ICT

.....
( )
b.p Ketua Setiausaha
Kementerian Pembangunan Wanita, Keluarga dan Masyarakat
Tarikh:.....

Lampiran 1

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER KPWKM

KEMENTERIAN PEMBANGUNAN WANITA,
KELUARGA DAN MASYARAKAT

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER KPWKM

Nama :

No. Kad Pengenalan :

Jawatan :

Bahagian / Unit :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
( )
b.p Ketua Setiausaha
Kementerian Pembangunan Wanita, Keluarga dan Masyarakat

Tarikh : .

Lampiran 2

LAMPIRAN 'C'

[Arahan Keselamatan (Semakan dan Pindaan) 2017]

PERAKUAN UNTUK DITANDATANGANI OLEH PEGAWAI AWAM BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 *[Akta 88]* dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana kerajaan dalam Malaysia, 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 perkhidmatan saya dengan Seri Paduka baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu medapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kerajaan.

Tandatangan :.....

Nama (huruf besar) :.....

No. Kad Pengenalan :.....

Jawatan :.....

Jabatan :.....

Tarikh :.....

Disaksikan oleh

_____

(Tandatangan)

Nama (huruf besar) :.....

No. Kad Pengenalan :.....

Jawatan :.....

Jabatan :.....

Tarikh :.....

Cap Jabatan :.....

Lampiran 2

LAMPIRAN 'E'

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia telah selesai.

Tandatangan : .....

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Organisasi : .....

Tarikh : .....

Disaksikan oleh _____

(Tandatangan)

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

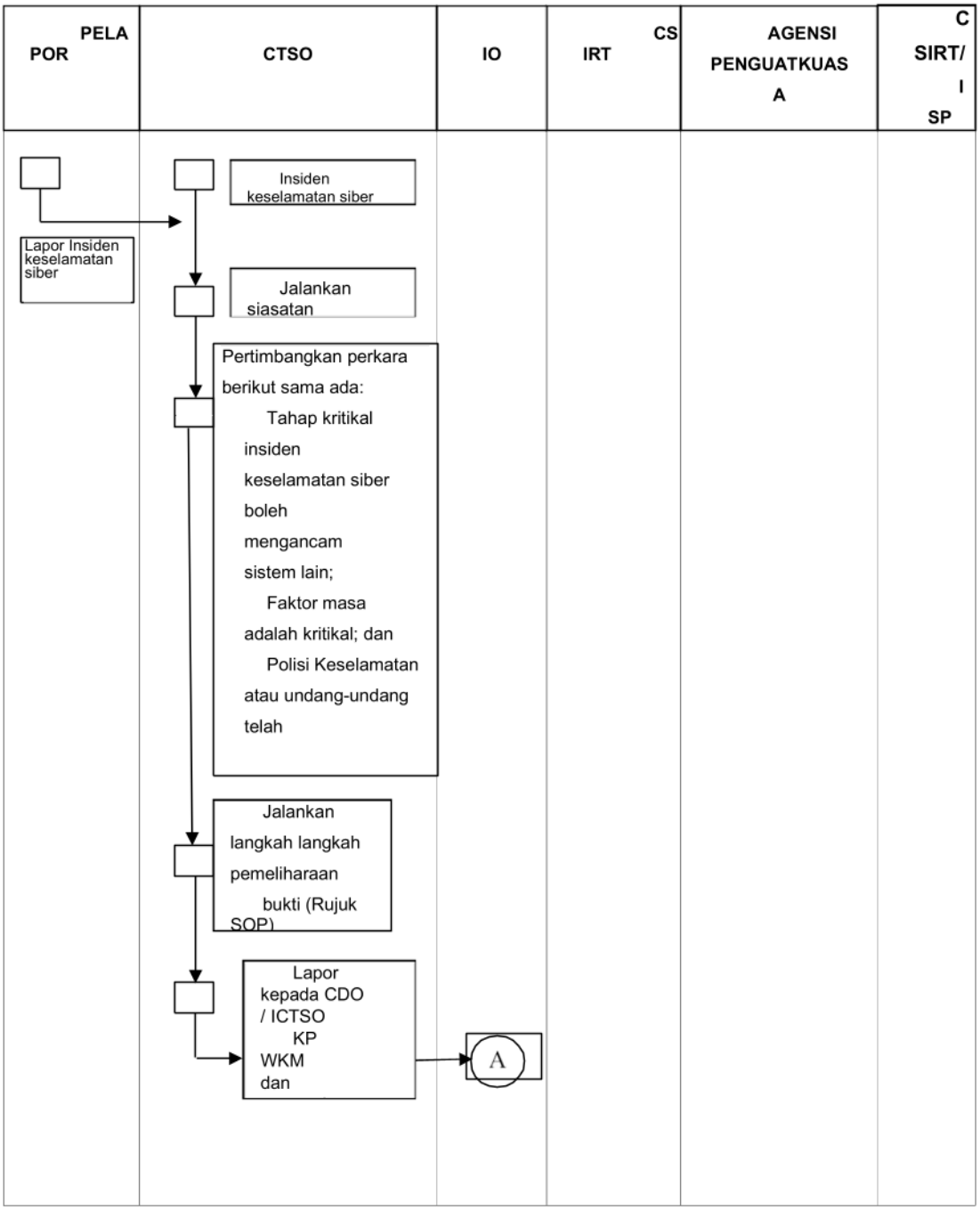
Jawatan : .....

Jabatan / Organisasi : .....

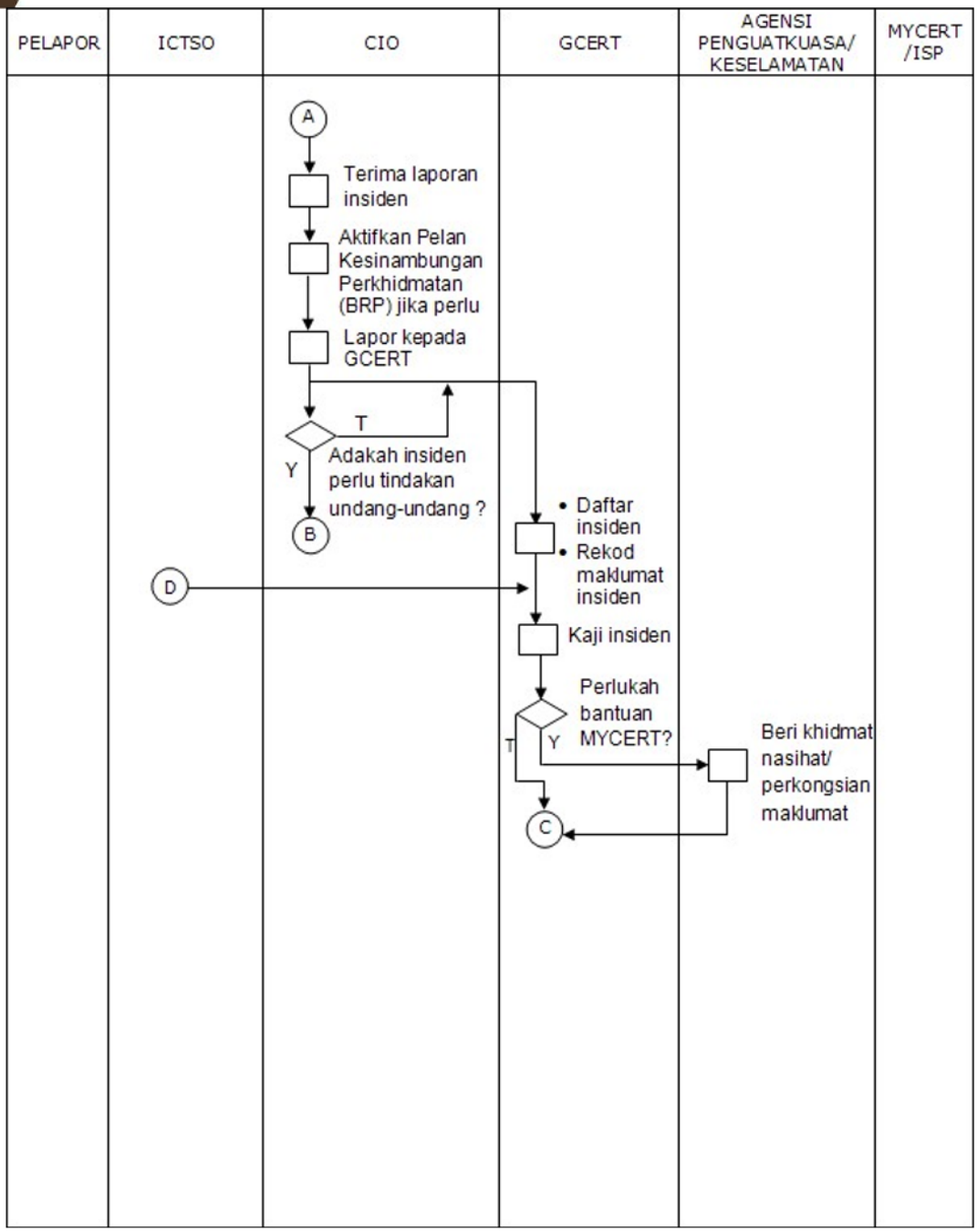
Tarikh : .....

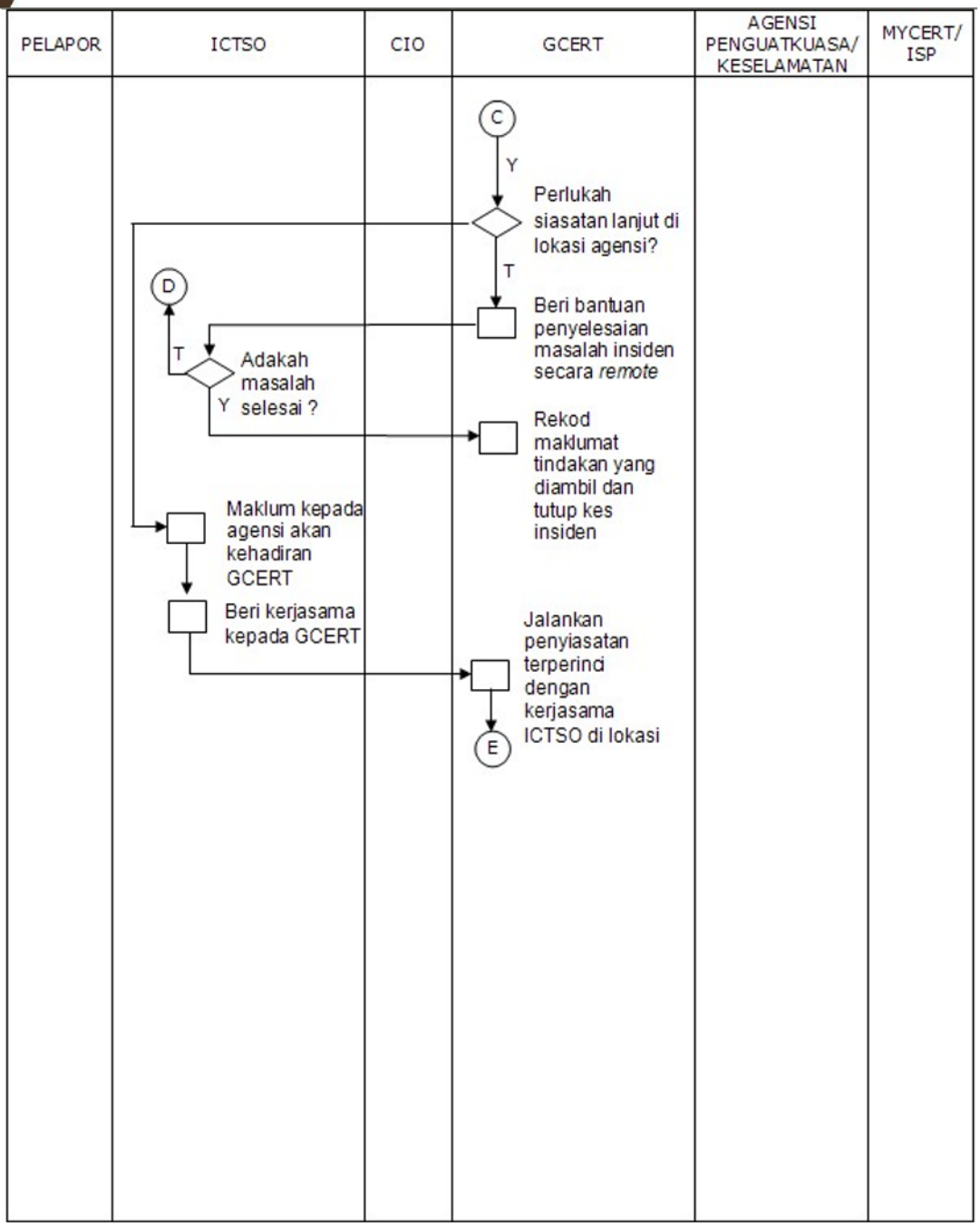
Cap Jabatan / Organisasi

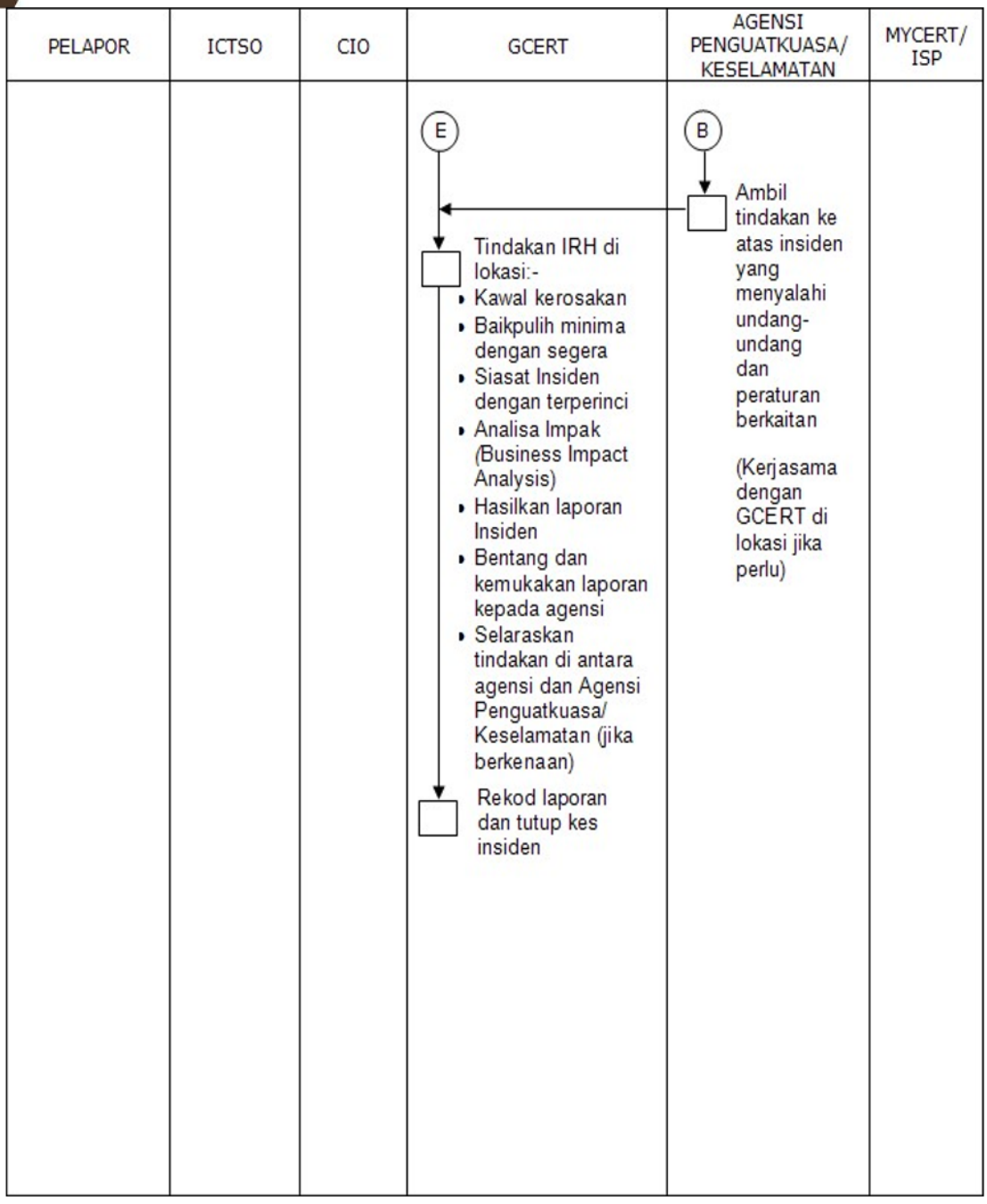
Lampiran 3



Rajah1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan Siber KPWKM dan Agensi


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT /ISP
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada GCERT
T
Y
Adakah insiden perlu tindakan undang-undang ?
B
D
• Daftar insiden
• Rekod maklumat insiden
Kaji insiden
Perlukah bantuan MYCERT?
T
Y
Beri khidmat nasihat/ perkongsian maklumat
C


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ ISP
C
Y
Perlukah siasatan lanjut di lokasi agensi?
T
Beri bantuan penyelesaian masalah insiden secara remote
D
T
Adakah masalah selesai ?
Y
Rekod maklumat tindakan yang diambil dan tutup kes insiden
Maklum kepada agensi akan kehadiran GCERT
Beri kerjasama kepada GCERT
Jalankan penyiasatan terperinci dengan kerjasama ICTSO di lokasi
E


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ ISP
E
B
Ambil tindakan ke atas insiden yang menyalahi undang-undang dan peraturan berkaitan
(Kerjasama dengan GCERT di lokasi jika perlu)
Tindakan IRH di lokasi:-
Kawal kerosakan
Baikpulih minima dengan segera
Siasat Insiden dengan terperinci
Analisa Impak (Business Impact Analysis)
Hasilkan laporan Insiden
Bentang dan kemukakan laporan kepada agensi
Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/ Keselamatan (jika berkenaan)
Rekod laporan dan tutup kes insiden

SENARAI PERUNDANGAN DAN PERATURAN

Lampiran 4

1.	Arahan Keselamatan;
2.	Perintah-Perintah Am;
3.	Arahan Perbendaharaan;
4.	Pekeliling Perbendaharaan (PP);
5.	Dasar Perkhidmatan Pengkomputeran;
6.	Garis Panduan Pengurusan Pusat Data Sektor Awam (PDSA);
7.	Polisi Keselamatan Siber JDN.
8.	Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam;
9.	Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (Gcert) Oleh Agensi Keselamatan Siber Negara (NACSA);
10.	Akta Rahsia Rasmi 1972;
11.	Akta Tandatangan Digital 1997;
12.	Akta Jenayah Komputer 1997;
13.	Akta Hak Cipta (Pindaan) Tahun 1997;

14.	Akta Komunikasi Dan Multimedia 1998;
15.	Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan;
16.	Malaysian Public Sector Management Of Information And Communications TechnologySecurity Handbook (MyMIS) 2002;
17.	Dasar Pengurusan Rekod Dan Arkib Elektronik 2003;
18.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet Dan Mel Elektronik Di Agensi-Agensi Kerajaan;
19.	Surat Pekeliling Am Bilangan 3 Tahun 2024 – Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024
20.	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;
21.	Arahan Teknologi Maklumat 2007;
22.	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) V1.0 April 2016;
23.	Pekeliling Am Bilangan 4 Tahun 2022 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT);
24.	Pekeliling Am Bil.4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Sektor Awam bertarikh 1 Ogos 2022;
25.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2021 – Dasar Perkongsian Data Sektor Awam
26.	Surat Pekeliling Am Bilangan 4 Tahun 2024 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam Yang Bertarikh 21 Mac 2024;
27.	Surat Pekeliling Am Bilangan 7 Tahun 2024 - Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek Teknologi Maklumat Dan Komunikasi (ICT) Agensi Sektor Awam.

28.	Cyber Security Act [Act 854]