KEMENTERIAN PENGANGKUTAN MALAYSIA

POLISI KESELAMATAN SIBER

KEMENTERIAN PENGANGKUTAN MALAYSIA (MOT)

KANDUNGAN

1. REKOD PINDAAN POLISI KESELAMATAN SIBER MOT

VERSI	TARIKH	KELULUSAN	TARIKH KUATKUASA	KETERANGAN PINDAAN
1.0	8 Jun 2023	JPICT MOT Bil. 3/2023 (3 Julai 2023)	12 Oktober 2023	Menggantikan Dasar Keselamatan ICT (2019)
2.0	28 Ogos 2024	JKP MOT Bil. 2/2024 (30 September 2024)	30 September 2024	Penambahan kawalan untuk: 1. PKSMOT - K04/05 Pelabelan Maklumat 2. PKSMOT - K04/07 Keselamatan Maklumat 3. PKSMOT - K04/08 Data Masking 4. PKSMOT - K08/07/05 Penyeragaman Jam (Clock Synchronization) 5. PKSMOT - K09/05 Keselamatan Perkhidmatan Rangkaian 6. PKSMOT - K09/06 Pengasingan Dalam Rangkaian 7. PKSMOT - K09/07 Pemindahan/Pertukaran Data dan Maklumat 8. PKSMOT - K09/07/01 Polisi dan Prosedur Pemindahan/Pertukaran Data dan Maklumat 9. PKSMOT - K09/07/02 Perjanjian Mengenai Pemindahan/Pertukaran Data dan Maklumat 10. PKSMOT - K09/08 Perjanjian Kerahsiaan atau Ketakdedahan 11. PKSMOT - K11/03 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal 12. PKSMOT - K11/04 Kawalan Keselamatan Maklumat Bagi Rantaian Bekalan ICT 13. PKSMOT - K11/05 Memantau dan Mengkaji Semula Perkhidmatan Pembekal 14. PKSMOT - K11/06 Menguruskan Perubahan Kepada Perkhidmatan Pembekal 15. Penambahan Kawalan 15 : Risikan Ancaman

				(Threat Intelligence) 16. Penambahan Kawalan 16. Penambahan Kawalan 16 : Keselamatan Maklumat bagi Penggunaan Perkhidmatan Cloud

2. PENGENALAN

Kementerian Pengangkutan (MOT) Malaysia berperanan untuk menyediakan perkhidmatan bagi perancangan, pembangunan dan pengurusan sumber manusia sektor awam yang cemerlang berteraskan profesionalisme, integriti dan teknologi. Dokumen ini diguna pakai oleh semua pengguna yang menyediakan perkhidmatan, mencapai dan menggunakan aset dan sistem aplikasi *Information and Communication Technology* (ICT) di MOT. Polisi Keselamatan Siber (PKS) MOT disediakan berpandu kepada piawaian antarabangsa iaitu ISO/IEC 27001:2022.

3. OBJEKTIF

Objektif utama PKS adalah seperti berikut:

1. Menerangkan kepada semua pengguna merangkumi warga MOT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT dan digital MOT mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber;

2. memastikan keselamatan penyampaian perkhidmatan MOT di tahap tertinggi sekaligus meningkatkan tahap keyakinan pihak-pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

3. memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT jabatan;

4. melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan daripada segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan;

5. meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;

6. meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan pihak luaran;

7. memperkemaskan pengurusan risiko;

8. mencegah penyalahgunaan atau kecurian aset ICT jabatan; dan

9. melindungi aset ICT daripada penyelewengan oleh pengguna dan pihak luaran.

4. PERNYATAAN POLISI

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

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

1. melindungi maklumat rahsia rasmi dan maklumat rasmi MOT dari capaian tanpa kuasa yang sah;

2. menjamin setiap maklumat adalah tepat dan sempurna;

3. memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

4. memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber-sumber yang sah.

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

1. Kerahsiaan – maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran.

2. Integriti – data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan.

3. Tidak boleh disangkal – punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.

4. Kesahihan – data dan maklumat hendaklah dijamin kesahihannya.

5. Kebolehsediaan – data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan 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.

5. SKOP

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

1. data dan maklumat termasuk *hardcopy* dan *softcopy* hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

2. semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan MOT.

Bagi menentukan sistem ICT ini terjamin keselamatannya sepanjang masa, PKS MOT ini merangkumi perlindungan ke atas semua bentuk maklumat ICT kerajaan yang dimasukkan, di wujud, di musnah, disimpan, dijana, dicetak, diakses, diedar dan yang dibuat salinan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. Data dan maklumat
   Semua data dan maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT.

2. Peralatan ICT
   Semua peralatan komputer seperti server, firewall, komputer peribadi, komputer desktop, pencetak, peralatan multimedia dan alat-alat prasarana seperti *Uninterruptible Power Supply* (UPS), punca kuasa dan lain-lain.

3. Media storan
   Semua media storan yang digunakan untuk menyimpan data dan maklumat seperti *optical disk, flash disk, hard disk, USB flash drive, catridge tape, compact disc* (CD) dan lain-lain.

4. Media komunikasi
   Semua peralatan berkaitan komunikasi seperti pelayan atau perkakasan rangkaian, *gateway, router*, *wireless* LAN, peralatan sidang video*, modem*,

kabel rangkaian, NIC, *switch* dan sebagainya.

5. Perisian

   Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat. Ini termasuklah sistem aplikasi seperti Portal MOT dan perisian sistem seperti Windows, LINUX dan perisian utiliti, perisian komunikasi, sistem pengurusan pangkalan data, fail program, fail data dan lain-lain.

6. Dokumentasi

   Semua dokumen termasuk prosedur dan manual pengguna yang berkaitan dengan aset ICT, dokumen pemasangan dan pengoperasian peralatan dan perisian.

7. Premis Komputer dan Komunikasi

   Semua kemudahan serta premis yang diguna untuk menempatkan perkara 1 hingga 6 di atas.

8. Manusia

   Semua pengguna yang dibenarkan.

9. Sumber Luaran

   Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi MOT. Contoh perkhidmatan sumber luaran ialah:

   a) Perisian Sebagai Satu Perkhidmatan (SaaS);
   b) Platform Sebagai Satu Perkhidmatan (PaaS);
   c) Infrastruktur Sebagai Satu Perkhidmatan (IaaS);
   d) Storan Pengkomputeran Awan (Cloud Storage); dan
   e) Pemantauan Keselamatan

10. Perkhidmatan

    Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan 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.

6. PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS MOT adalah seperti berikut:

1. 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.

2. Hak Akses Minimum
   Hak akses kepada pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah dan menghapuskan sesuatu data atau maklumat.

3. Kebertanggungjawaban atau Akauntabiliti
   Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Bagi menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

4. Pengasingan
   Tugas mewujud, menghapus, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (*unauthorized access*) serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi data, operasi, pangkalan data dan rangkaian.

5. Pengauditan
   Tujuan aktiviti ini ialah untuk mengenal pasti insiden keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Dengan itu, semua log yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit.

6. Pematuhan

   PKS MOT hendaklah dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

7. Pemulihan

   Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui proses penduaan (*backup*) dan mewujudkan Pelan Pemulihan Bencana (DRP) di bawah Pengurusan Kesinambungan Perkhidmatan (PKP).

8. Saling Bergantung

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

7. PENILAIAN RISIKO KESELAMATAN ICT

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

MOT hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan 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 MOT termasuk aplikasi, perisian, perkakasan, pelayan, rangkaian, pangkalan data, sumber manusia, proses, dan prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuk pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

MOT bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 3 Tahun2024 : Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam yang dikeluarkan oleh Agensi Keselamatan Siber Negara (NACSA).

MOT perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan melaksanakan tindakan berikut;

a) Kerentanan (*Vulnerability*)
   Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

b) Ancaman (*threat*)
   MOT hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

c) Impak (*Impact*)

MOT hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi MOT.

d) Tahap Risiko

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

e) Penguraian Risiko

Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/ faedahnya.

Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

- Teknologi

  Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, firewall digunakan untuk menghadkan capaian logikal kepada sistem tertentu.

- Proses

  Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

- Manusia

  Mengenal pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

f) Pengurusan Risiko

Penyedia perkhidmatan digital di MOT hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

- mengenal pasti kerentanan;
- mengenalpasti ancaman;
- menilai risiko;
- menentukan penguraian risiko;
- memantau keberkesanan penguraian risiko; dan
- memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun oleh Bahagian/Jabatan masing-masing dan dimaklumkan kepada Ketua Jabatan atau Jawatankuasa yang ditentukan oleh Ketua Jabatan.

8. PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Setiap projek di MOT hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.

Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), Polisi Keselamatan Siber MOT dan surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.

Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, data-dalam- pergerakan, data dalam-simpanan dan menghalang ketirisan data.

Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

1. Peranti Pengkomputeran Peribadi

   Peranti Pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, komputer *desktop*, telefon pintar, tablet dan peranti storan.

2. Peranti Rangkaian

   a. Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch*, *router*, *firewall*, peranti VPN dan kabel.

   b. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam- pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat

3. Aplikasi

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

b. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

4. Pelayan

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

b. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam- penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

5. Persekitaran Fizikal

a. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

b. MOT hendaklah merujuk ke Pejabat Ketua Pegawai Keselamatan Kerajaan untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

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

d. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam- penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

KAWALAN 01 : POLISI KESELAMATAN MAKLUMAT

PKSMOT - K01 **Objektif**		
PKS MOT ini diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran operasi jabatan secara berterusan, meminimumkan kerosakan atau kemusnahan aset-aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, integriti, tidak boleh disangkal, keboleh sediaan dan kesahihan.		
PKSMOT-K01/01 Pelaksanaan Polisi		
	Pelaksanaan polisi ini akan dijalankan oleh Ketua Setiausaha MOT, dan dibantu oleh Jawatankuasa Pemandu ICT (JPICT) dan Jawatankuasa Pengurusan ISMS.	Ketua Setiausaha MOT
PKSMOT-K01/02 Penyebaran Polisi		
	Polisi ini perlu disebarkan kepada semua yang terlibat dengan infrastruktur ICT meliputi semua pengguna.	ICTSO
PKSMOT-K01/03 Penyelenggaraan Polisi		
	PKS MOT adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan PKS MOT: a. mengenal pasti dan menentukan perubahan yang diperlukan; b. mengemukakan cadangan pindaan secara bertulis untuk persetujuan dan pengesahan Jawatankuasa Pemandu Projek ISMS; c. memaklumkan pindaan yang telah disahkan kepada semua pengguna; d. menyemak semula dokumen sekurang-kurangnya setahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	ICTSO
PKSMOT-K01/04 Pematuhan Polisi		
	PKS MOT mestilah dipatuhi oleh semua pengguna.	Pengguna

KAWALAN 02 : ORGANISASI KESELAMATAN MAKLUMAT

PKSMOT - K02 Objektif		
Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS MOT.		
PKSMOT-K02/01 Tadbir Urus Keselamatan Maklumat		
PKSMOT-K02/01/01 Ketua Setiausaha MOT		
	Peranan dan tanggungjawab Ketua Setiausaha MOT adalah seperti berikut: a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah PKS MOT; b. Memastikan semua pengguna mematuhi PKS MOT; c. Memastikan semua keperluan jabatan seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan adalah mencukupi; dan d. Memastikan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam PKS MOT.	Ketua Setiausaha MOT
PKSMOT-K02/01/02 Ketua Pegawai Digital (CDO) / Ketua Pegawai Maklumat (CIO)		
	Jawatan Ketua Pegawai Digital (CDO) / Ketua Pegawai Maklumat (CIO) adalah disandang oleh Timbalan Ketua Setiausaha (Pengurusan) MOT. Peranan dan tanggungjawab CDO/CIO adalah seperti berikut: a. bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MOT; b. bertanggungjawab menyelaras dan mengurus pelan tindakan dan program keselamatan seperti penyediaan PKS MOT, pelan latihan dan kesedaran pengguna, pengurusan risiko dan pengauditan; dan c. menentukan keperluan keselamatan ICT.	CDO/CIO

PKSMOT-K02/01/03 Pengurus ICT		
	Jawatan Pengurus ICT disandang oleh Setiausaha Bahagian, Bahagian Pengurusan Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. memastikan PKS MOT dilaksanakan dan dipatuhi di bahagian; b. memastikan semua pengguna di MOT mematuhi polisi, piawaian dan garis panduan keselamatan ICT, dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT; c. mengkaji semula aspek-aspek keselamatan fizikal berkaitan ICT; d. memastikan keperluan PKS dilaksanakan dalam operasi semasa seperti berikut: i. pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; ii. pembelian atau peningkatan perisian dan sistem komputer; iii. perolehan teknologi dan perkhidmatan komunikasi baharu; iv. pelantikan pembekal, perunding atau rakan usaha sama; dan v. menentukan pembekal, perunding atau rakan usaha sama menjalani tapisan keselamatan selaras dengan keperluan tahap perkhidmatan. e. menyemak dan mengesahkan garis panduan, prosedur dan tatacara bagi semua aplikasi yang dibangunkan di bahagian-bahagian agar mematuhi keperluan PKS MOT;	Pengurus ICT

	f. memastikan dokumen Pelan Pemulihan Bencana (DRP) diwujudkan dan dilaksanakan; g. memastikan sistem kawalan capaian pengguna ke atas aset-aset ICT MOT dilaksanakan; h. memastikan aspek keselamatan maklumat dilaksanakan dalam setiap pengurusan projek; dan i. mempengerusikan Mesyuarat Pasukan Tindak Balas Insiden Keselamatan ICT MOT (CSIRT MOT).	
PKSMOT-K02/01/04	**Pegawai Keselamatan ICT (ICTSO)**	
	Jawatan Pegawai Keselamatan ICT (ICTSO) adalah disandang oleh Ketua Penolong Setiausaha, Unit Operasi dan Keselamatan ICT (OKI), Bahagian Pengurusan Maklumat. Peranan dan tanggungjawab ICTSO adalah seperti berikut: a. mengurus keseluruhan program keselamatan ICT MOT; b. menguatkuasakan pelaksanaan PKS MOT di semua bahagian di MOT; c. memastikan pengurusan risiko dan audit keselamatan ICT berpandukan dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) untuk mengenal pasti ketidakpatuhan kepada PKS MOT; d. mencadangkan langkah-langkah pengukuhan bagi mematuhi dasar-dasar berkaitan keselamatan ICT MOT; e. melaporkan insiden keselamatan ICT kepada pihak *National Cyber Security Agency* (NACSA) dan seterusnya membantu dalam penyiasatan atau pemulihan;	ICTSO

	f. memastikan program-program kesedaran mengenai keselamatan ICT dilaksanakan; g. menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman kepada keselamatan ICT dan menyediakan khidmat nasihat serta langkah pemulihan yang bersesuaian; h. melaporkan insiden keselamatan ICT kepada CDO/CIO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan; i. memastikan pematuhan PKS MOT oleh pihak luaran yang memberi perkhidmatan ICT kepada MOT untuk tujuan pembekalan, pemasangan, penyelenggaraan dan sebagainya; j. menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT; k. memastikan PKS MOT dikemas kini sesuai dengan perubahan teknologi, arahan jabatan dan ancaman-ancaman dari semasa ke semasa; dan memastikan Pelan Strategik Pendigitalan MOT mengandungi aspek keselamatan ICT.	
PKSMOT-K02/01/05	**Pentadbir Sistem**	
	Pentadbir Sistem terdiri daripada seperti berikut: a. Pentadbir Rangkaian; b. Pentadbir Keselamatan; c. Pentadbir Portal (Webmaster); d. Pentadbir Pusat Data; e. Pentadbir Sistem Aplikasi; f. Pentadbir E-mel; g. Pentadbir Media Sosial dan Aplikasi Sosial MOT; dan h. Pegawai Aset ICT.	Pentadbir Sistem

PKSMOT-K02/01/06 Pentadbir Rangkaian		
	Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: a. memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di MOT beroperasi sepanjang masa; b. memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; c. merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d. mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; e. memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian MOT secara tidak sah seperti melalui peralatan modem dan *dial-up*; dan f. memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian.	Pentadbir Rangkaian

PKSMOT-K02/01/07 Pentadbir Keselamatan		
	Peranan dan tanggungjawab Pentadbir Rangkaian Dan Keselamatan adalah seperti berikut: a. merancang peningkatan dan keselamatan infrastruktur sedia ada; b. melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT; c. memastikan keselamatan infrastruktur ICT sentiasa berada dalam ketersediaan yang tinggi untuk melindungi aset ICT; d. memastikan semua kawalan keselamatan mematuhi dasar-dasar berkaitan keselamatan ICT MOT; dan e. memantau keselamatan penggunaan aset dan sistem dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan.	Pentadbir Keselamatan
PKSMOT-K02/01/08 Pentadbir Portal (Web Master)		
	Peranan dan tanggungjawab Pentadbir Portal adalah seperti berikut: a. menerima kandungan portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b. memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar; c. memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka portal; d. mengasingkan kandungan dan aplikasi dalam talian untuk capaian secara Intranet dan Internet ke portal MOT; e. memastikan hanya maklumat yang bersifat terbuka dipaparkan di portal;	Pentadbir Portal (*Web Master*)

	f. memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; g. melaksanakan perkemasan keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; h. memantau proses *backup* dan *restoration* ke atas kandungan dan aplikasi portal; dan i. melaporkan sebarang pelanggaran keselamatan portal kepada ICTSO.	
PKSMOT-K02/01/09 Pentadbir Pusat Data		
	Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: a. memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; b. memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; c. melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem; d. melaporkan sebarang pelanggaran keselamatan Pusat Data MOT kepada ICTSO; dan e. memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.	Pentadbir Pusat Data
PKSMOT-K02/01/10 Pentadbir Sistem Aplikasi		
	Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: a. mengkaji cadangan pembangunan atau penyelarasan sistem atau modul di MOT; b. melaksanakan kajian semula serta memperbaiki sistem atau modul sedia ada di MOT;	Pentadbir Sistem Aplikasi

	c. membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem atau modul di MOT; d. melaksanakan pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa; e. bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem atau modul; f. menyediakan dokumentasi sistem atau modul dan manual pengguna; g. memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; h. memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; i. memastikan *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi terkemas kini supaya terhindar daripada ancaman virus dan penggodam; j. mematuhi dan melaksanakan prinsip-prinsip PKS dalam perwujudan akaun pengguna ke atas setiap sistem aplikasi; k. mengehadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya; dan l. melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya.	

PKSMOT-K02/01/11 Pentadbir E-mel		
	Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut: a. menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b. pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c. memastikan pengguna e-mel MOT berkemahiran menggunakan e-mel dan melaksanakan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan. d. memastikan kemudahan e-mel dapat dicapai melalui pelbagai peralatan ICT dan alat komunikasi; e. mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan; dan f. memastikan maklumat perhubungan e-mel pengguna perlu dikemas kini dari semasa ke semasa.	Pentadbir E-mel
PKSMOT-K02/01/12 Pentadbir Media Sosial dan Aplikasi Sosial MOT		
	Peranan dan tanggungjawab Pentadbir Media Sosial dan Aplikasi Sosial MOT adalah seperti berikut: a. memaklumkan kepada semua ahli kumpulan, sebab utama kumpulan aplikasi pesanan diwujudkan dan memikirkan sama ada peraturan asas diperlukan; b. prihatin terhadap peraturan atau syarat-syarat yang digariskan oleh penyedia platform; c. menegur *posting* atau komen untuk memastikan perbincangan berada di landasan yang betul;	Pentadbir Media Sosial dan Aplikasi Sosial MOT

	d. sentiasa semak *posting* atau komen (dengan seorang *moderator*, jika boleh); e. mempertimbangkan untuk mengeluarkan atau menyekat mereka yang terus membuat *posting* atau komen jelik; f. menggunakan platform untuk menyampaikan informasi yang tepat dan terkini; g. menjalankan kajian untuk mengetahui pendapat dan maklum balas daripada pengikut media sosial; h. membuat strategi agar maklumat yang betul disampaikan boleh disebarkan secara meluas dan teratur; dan i. memberi maklum balas kepada sebarang pertanyaan dan keraguan yang ditinggalkan di platform media sosial dalam jangka masa yang bersesuaian.	
PKSMOT-K02/01/13 Pegawai Aset ICT		
	Pegawai Aset ICT ialah pegawai yang dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab Pegawai Aset ICT adalah seperti berikut: a. memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan; b. memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan/ Bahagian; c. memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset;	Pegawai Aset ICT

	d. memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua Jabatan/ Pegawai Aset/ Pegawai- pegawai lain yang diberi kuasa oleh Ketua Jabatan; e. memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ naik-taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira; f. memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama MOT/ Bahagian/ Agensi berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan; g. memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan; h. memastikan senarai daftar induk aset ICT Kerajaan disediakan; i. memastikan senarai aset ICT Kerajaan disediakan dipaparkan mengikut lokasi; j. memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan; k. bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan; l. merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya sekali setahun; dan m. memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.	

PKSMOT-K02/01/14	Pengguna	
	Pengguna terdiri daripada warga MOT dan pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan. Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Pengguna perlu membaca, memahami dan mematuhi PKS MOT; b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d. melaksanakan prinsip-prinsip PKS dan menjaga kerahsiaan maklumat MOT; e. melaksanakan langkah-langkah perlindungan seperti berikut: i) menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii) memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii) memastikan maklumat sedia untuk digunakan; iv) menjaga kerahsiaan kata laluan; v) mematuhi piawaian, prosedur, langkah, pekeliling dan garis panduan keselamatan ICT yang ditetapkan; vi) melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii) menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;	Pengguna

	g. menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. mengawal aktiviti penggunaan media sosial dan aplikasi sosial seperti di bawah: i) mengelakkan ketirisan maklumat; ii) tidak memberi atau mendedahkan sebarang komen atau pernyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan; iii) tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasi sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan iv) tidak menggunakan saluran media sosial atau media sosial hingga mengganggu fokus dalam urusan kerja. i. menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber MOT seperti di **Lampiran 1.**	
PKSMOT-K02/01/15	**Jawatankuasa Pemandu ICT (JPICT) MOT**	
	Keanggotaan JPICT adalah seperti berikut: Pengerusi: Ketua Setiausaha atau Pegawai Yang Diberi Kuasa Ahli: a. Ketua Bahagian di bawah Kementerian; b. Ketua Pegawai Digital (CDO) Kementerian; c. Pengurus ICT Kementerian/Jabatan/Agensi; d. Ketua Jabatan/Agensi atau Ketua Pegawai Digital (CDO) Jabatan; e. Ketua Pegawai Keselamatan ICT (ICTSO) Kementerian; dan f. Ahli-ahli jemputan yang berkaitan Urus setia: Bahagian Pengurusan Maklumat, MOT	Ketua Setiausaha atau Pegawai Yang Diberi Kuasa

	Bidang kuasa: a. menetapkan hala tuju dan strategi ICT untuk pembangunan dan pelaksanaan projek ICT MOT; b. mengesahkan cadangan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan projek ICT MOT dan semua agensi di bawahnya; c. merancang, menyelaras dan menyeragamkan pembangunan dan pelaksanaan projek ICT MOT dan semua agensi di bawahnya supaya selaras dengan Pelan Strategik MOT, Pelan Strategik Pendigitalan MOT, Pelan Strategik Pendigitalan Sektor Awam (PSPSA) atau pelan yang setara; d. menilai dan melulus semua cadangan perolehan ICT MOT dan agensi di bawahnya berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan; e. menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi MOT dan semua agensi di bawahnya kepada JTISA untuk kelulusan teknikal berdasarkan had nilai yang ditetapkan; f. memastikan pelaksanaan projek ICT dipantau dan dilaporkan melalui sistem yang disediakan oleh JDN; g. mempromosi dan menggalakkan perkongsian pintar aplikasi ICT antara MOT dan semua agensi di bawahnya; h. meluluskan dasar/aktiviti keselamatan ICT MOT dan agensi di bawahnya; dan i. memastikan keselarasan projek ICT agar tiada duplikasi dan pembaziran.	

PKSMOT-K02/01/16 Pasukan Tindak Balas Insiden Keselamatan Siber MOT (CSIRTMOT)		
	Keanggotaan CSIRT MOT adalah seperti berikut: Pengerusi: Pengurus ICT, MOT Ahli : a. ICTSO MOT dan Agensi; b. Pegawai Teknologi Maklumat, Bahagian Pengurusan Maklumat, MOT; dan c. Penolong Pegawai Teknologi Maklumat, Bahagian Pengurusan Maklumat, MOT Peranan dan tanggungjawab CSIRT MOT adalah seperti berikut : a. Menerima dan mengesan aduan keselamatan ICT daripada GCERT serta menilai tahap dan jenis insiden; b. Merekodkan dan menjalankan siasatan awal insiden yang diterima dari GCERT; c. Menangani tindak balas *(responsive)* insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d. Menghubungi dan melapor insiden yang berlaku kepada NACSA sama ada sebagai input atau untuk tindakan seterusnya melalui laman web https://www.nacsa.gov.my; e. Menasihat agensi-agensi dibawah kawalan mengambil tindakan pemulihan dan pengukuhan; f. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Warga MOT; dan g. Menasihat agensi-agensi dibawah kawalan mengambil tindakan pemulihan dan pengukuhan.	CSIRT MOT

PKSMOT-K02/01/17	Pengurusan Kesinambungan Perkhidmatan (PKP)	
	Pengurusan Kesinambungan Perkhidmatan (PKP) merupakan proses pengurusan holistik yang mengenal pasti ancaman dan risiko, impak ancaman dan risiko tersebut terhadap fungsi kritikal MOT, dan penentuan strategi bagi memastikan perkhidmatan MOT dapat diteruskan walaupun berlaku gangguan atau bencana. MOT hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan keselamatan maklumat dalam situasi kecemasan contohnya semasa krisis atau bencana. Dalam merancang keselamatan maklumat, MOT perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberi kesan atas sistem penyampaian perkhidmatan dan fungsi MOT. MMOT perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan dan keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) MOT; b. Menetapkan polisi PKP; c. Mengenal pasti perkhidmatan kritikal; d. Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindakan Balas Kecemasan dan Pelan Pemulihan Bencana ICT; e. Melaksanakan program kesedaran dan latihan pasukan PKP dan warga MOT; f. Melaksanakan simulasi ke atas dokumen di DRP; dan g. Melaksanakan penyelenggaraan ke atas pelan DRP. PKP melibatkan 3 pasukan pengurusan iaitu: a. Pasukan Tindak Balas Kecemasan (ERT – *Emergency Response Team*)	Koodinator PKP, Pasukan Tindak Balas Kecemasan (ERT – *Emergency Response Team*), Pasukan Pemulihan Bencana ICT (DRT – *Disaster Recovery Team*), Pasukan Pemulihan Bencana ICT, Pasukan Komunikasi Krisis (CCT- *Communication Crisis Team*)

	• Menyediakan dan melaksanakan perancangan yang sistematik bagi memastikan tindakan segera dalam mengawal kejadian kecemasan di MOT dijalankan secara strategik lagi efektif. • Pasukan ERT diurus setia oleh Bahagian Pentadbiran, MOT b. Pasukan Pemulihan Bencana ICT (*ICT DRT – Disaster Recovery Team*) • Menyediakan, mengurus dan melaksanakan proses pemulihan perkhidmatan ICT yang terganggu akibat bencana yang berlaku. • Melaksanakan penilaian risiko dan analisis impak perkhidmatan bagi fungsi kritikal yang telah dikenal pasti. • Pasukan DRT diketuai oleh Bahagian Pengurusan Maklumat, MOT. c. Pasukan Komunikasi Krisis (CCT- *Communication Crisis Team*) • Menyediakan dan melaksana polisi dan prosedur untuk mengkoordinasi makluman kepada orang awam, ahli keluarga dan saudara mara warga MOT mengenai keadaan mereka apabila berlaku bencana luar jangka. • Pasukan CCT diketuai oleh Unit Komunikasi Korporat, MOT.	

PKSMOT-K02/02 Pihak Luaran		
PKSMOT-K02/02/01 Keperluan Keselamatan Dalam Perkhidmatan ICT		
	Pihak Luaran terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan atau pelawat yang mengunjungi MOT atas urusan rasmi. Perkara yang perlu dipatuhi adalah seperti berikut: a. Membaca, memahami dan mematuhi PKS MOT b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada Pembekal dan Pihak Ketiga d. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan Pembekal dan Pihak Ketiga. Perkara-perkara berikut hendaklah dilaksanakan dan dipatuhi tertakluk kepada skop/bidang tugas yang berkaitan e. Pematuhan PKS MOT; f. Tapisan Keselamatan; g. Arahan Teknologi Maklumat 2007 (IT Instructions); h. Perakuan Akta Rahsia Rasmi 1972; i. Hak Harta Intelek; j. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; k. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna; l. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber MOT seperti di **Lampiran 1**.	ICTSO, PICT, Pentadbir Sistem, Pentadbir Rangkaian, Pentadbir Keselamatan, Pentadbir Portal (*Web Master*), Pentadbir Pusat Data, Pentadbir Sistem Aplikasi, Pegawai Aset ICT, Pembekal, Pihak Ketiga

KAWALAN 03 : KESELAMATAN SUMBER MANUSIA

PKSMOT - K03	**Objektif**	
Memastikan semua pengguna yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam melindungi keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.		
PKSMOT - K03/01 Sebelum Perkhidmatan		
	Memastikan semua pengguna yang berkepentingan memahami tanggungjawab masing-masing dalam melindungi keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: a. menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua pengguna yang berkepentingan dalam menjamin keselamatan ICT sebelum, semasa dan selepas perkhidmatan; b. lulus tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika semasa yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; c. memastikan semua pengguna menandatangani Surat Akuan Pematuhan PKS MOT seperti di **Lampiran 1** dan Perakuan Akta Rahsia Rasmi 1972 [Akta 88] seperti di **Lampiran 2**; dan d. mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengurus ICT

PKSMOT - K03/02 Semasa Perkhidmatan		
	Memastikan semua pengguna yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong PKS MOT dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi termasuk yang berikut: a. memastikan semua pengguna yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan MOT; b. memastikan latihan dan program kesedaran yang berkaitan keselamatan ICT diberikan kepada pengguna dari semasa ke semasa; c. memastikan pelaksanaan latihan jabatan sentiasa mematuhi Pekeliling Perkhidmatan semasa yang berkuat kuasa (Dasar Latihan Sektor Awam), dan perancangan latihan jabatan bersesuaian dengan fungsi serta tugas-tugas semasa pengguna; d. memantapkan pengetahuan berkaitan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT; dan e. memastikan adanya tindakan tatatertib dan/atau perundangan ke atas semua pengguna sekiranya berlaku pelanggaran keselamatan maklumat jabatan.	Pengurus ICT

PKSMOT - K03/03 Bertukar Atau Tamat Perkhidmatan		
	Memastikan pertukaran atau tamat perkhidmatan semua pengguna yang berkepentingan diuruskan dengan teratur. Perkara yang perlu dipatuhi termasuk: a. memastikan semua aset ICT dikembalikan kepada Bahagian Pengurusan Maklumat, MOT mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b. membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan MOT dan/atau terma perkhidmatan.	Pengurus ICT

KAWALAN 04 : PENGURUSAN ASET

PKSMOT - K04	**Objektif**	
Memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT MOT.		
PKSMOT - K04/01	**Akauntabiliti Aset ICT**	
	Memberi kawalan dan sokongan perlindungan yang bersesuaian ke atas semua aset ICT MOT. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: a. memastikan semua aset ICT dikenal pasti, dikelaskan, didokumenkan, diselenggarakan dan dilupuskan. Maklumat aset direkodkan dan dikemas kini dalam Sistem Pengurusan Aset (SPA), Kad Daftar Harta Modal dan Aset Alih Bernilai Rendah sebagaimana mengikut Pekeliling Perbendaharaan AM 2 Tahun 2018: Tatacara Pengurusan Aset Alih Kerajaan atau senarai aset yang berkaitan; b. memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MOT; d. memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan; e. setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan f. penggunaan aset ICT MOT mestilah tujuan tugas rasmi sahaja.	Pegawai Aset ICT, Pengguna

PKSMOT - K04/02	Peminjaman dan Pemulangan Aset ICT	
	Peminjaman Langkah-langkah perlu diambil adalah seperti berikut: a. mendapatkan kelulusan mengikut peraturan yang telah ditetapkan bagi membawa keluar peralatan bagi tujuan yang dibenarkan; b. melindungi dan mengawal peralatan sepanjang masa; c. merekodkan aktiviti peminjaman dan pemulangan peralatan; dan d. menyemak peralatan ketika peminjaman dan pemulangan dilakukan. **Pemulangan** Memastikan semua aset ICT dikembalikan mengikut peraturan dan atau terma perkhidmatan yang ditetapkan bagi pegawai yang: a. bertukar keluar; b. bersara; c. ditamatkan perkhidmatan; dan d. diarahkan oleh Ketua Jabatan. Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.	Pegawai Aset ICT

PKSMOT - K04/03	**Pengelasan Maklumat**	
	Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada MOT. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan dan dilabel sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Pegawai Pengelas
PKSMOT - K04/04	**Pengendalian Maklumat**	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. menentukan maklumat sedia untuk digunakan; d. menjaga kerahsiaan kata laluan; e. mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; f. melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; g. menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum; dan h. mewujudkan salinan pendua maklumat penting bagi mengurangkan risiko kehilangan dan kemusnahan.	Pengguna

PKSMOT - K04/05	Pelabelan Maklumat	
	Maklumat hendaklah dilabelkan sewajarnya. Penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan Kerajaan yang sedang berkuatkuasa seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad	Pengguna
PKSMOT - K04/06	**Pengelasan dan Pengendalian Data Terbuka**	
	Data Terbuka ialah data yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan. Jabatan akan menyediakan set data terbuka berdasarkan bidang atau sektor atau kluster. Kategori set data ini tidak terhad dan boleh berubah mengikut fungsi teras dan keperluan semasa Jabatan. Data terbuka yang telah diperakukan akan diterbitkan ke Portal Data Terbuka Sektor Awam (DTSA) di bawah pengurusan JDN.	Pengurus ICT
PKSMOT - K04/07	**Keselamatan Maklumat**	
	Keselamatan maklumat penting bagi perlindungan data-dalam-penggunaan, data-dalam-pergerakan, data-dalam- simpanan dan menghalang ketirisan data. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat terperingkat hanya boleh dilakukan penduaan dan penyalinan pada media storan oleh Pengguna yang dibenarkan dengan kebenaran Ketua Jabatan/Pegawai Keselamatan Jabatan;	Ketua Jabatan Pegawai Keselamatan Jabatan, Pengguna

	(b) Menggunakan teknologi enkripsi dan lain-lain kaedah keselamatan yang bersesuaian ke atas maklumat terperingkat yang disediakan dan dihantar secara elektronik; dan (c) Semua maklumat terperingkat hendaklah dihapuskan mengikut prosedur pelupusan semasa yang sedang berkuatkuasa dengan kelulusan Ketua Pengarah Arkib Negara.	
PKSMOT - K04/08	**Data Masking**	
	Data Masking ialah teknik yang digunakan untuk mencipta versi data yang kelihatan secara struktur seperti yang asal tetapi menyembunyikan maklumat sensitif. Versi dengan maklumat bertopeng kemudiannya boleh digunakan untuk pelbagai tujuan, seperti latihan pengguna atau ujian perisian. Objektif utama menyembunyikan data adalah untuk mencipta pengganti berfungsi yang tidak mendedahkan data sebenar. Data yang sepatutnya ditutup ialah: (a) Personal Identifiable Information (PII) Data yang boleh digunakan untuk mengenal pasti individu tertentu. Ini termasuk maklumat seperti nama penuh, nombor pasport, nombor lesen memandu dan nombor keselamatan sosial.	Pengguna

PKSMOT - K04/09 Pengendalian Media		
PKSMOT - K04/09/01 Media Storan		
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *optical disk, flash disk, hard disk, USB flash drive, catridge tape*, *compact disc* (CD). Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil: a. semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan; b. bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan dengan mendapat kelulusan pemilik maklumat terlebih dahulu; c. semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat sama ada dilaksanakan dalam bentuk/kaedah pemusnahan fizikal dan/ atau sanitasi data; d. Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa. e. semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti *(data safe)* yang mempunyai ciri-ciri keselamatan termasuk tahan daripada dipecahkan, api, air dan medan magnet; f. storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang lebih privasi dan tidak terbuka kepada umum. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;	Pentadbir Sistem, Pengguna

	g. akses dan pergerakan kepada media storan perlu direkodkan; h. perkakasan *backup* hendaklah diletakkan di tempat yang selamat dan terhad kepada pengguna yang dibenarkan sahaja; i. salinan atau *backup* pada media storan kedua hendaklah diadakan mengikut prosedur pengoperasian pusat data bagi tujuan keselamatan dan bagi mengelakkan kehilangan data dan seterusnya disimpan secara off site di lokasi yang telah ditetapkan; dan j. sebarang kehilangan data terperingkat di dalam media storan yang berlaku hendaklah dilaporkan kepada ICTSO dengan segera.	

KAWALAN 05 : KAWALAN CAPAIAN

PKSMOT - K05 **Objektif**		
Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT.		
PKSMOT-K05/01	**Kawalan Capaian**	
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong polisi kawalan capaian pengguna sedia ada.	Pentadbir Sistem
PKSMOT-K05/02	**Pengurusan Capaian Pengguna**	
PKSMOT-K05/02/01	**Pendaftaran Pengguna**	
	Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut dengan merujuk *Prosedur Operasi Standard* (SOP) - Pengurusan Pengguna Portal/Sistem Aplikasi Kementerian. a. akaun yang diperuntukkan oleh kementerian sahaja boleh digunakan; b. akaun *user id* hendaklah mencerminkan identiti pengguna; c. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan kementerian. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; d. penggunaan akaun milik orang lain adalah dilarang; e. akaun yang dikongsi bersama adalah dilarang kecuali yang dibenarkan oleh CIO/CDO/Pengurus ICT atau ICTSO; dan f. pengguna boleh disekat akses disebabkan kesalahan melanggar PKS MOT berdasarkan arahan oleh CIO/CDO/Pengurus ICT atau ICTSO.	Pentadbir Sistem, Pengguna

PKSMOT-K05/02/02	**Hak Capaian**	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui *(need-to-know-basis).* Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja.	Pentadbir Sistem
PKSMOT-K05/02/03	**Pengurusan Kata Laluan**	
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MOT seperti berikut: a. dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik) dan aksara khas; c. Mengelak penggunaan semula empat (4) kata laluan yang telah digunakan dalam tempoh 4 bulan. d. kata laluan mestilah ditukar setiap tiga puluh (30) hari, tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. kata laluan sistem pengoperasian (*OS*) atau *Directory Service* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f. kata laluan digalakkan ditukar secara kerap, tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun; g. kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; h. kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;	Pentadbir Sistem, Pengguna

	i. kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; j. kata laluan hendaklah disimpan dalam bentuk yang telah disulitkan *(encrypted)* atau di dalam file konfigurasi yang dibenarkan ; k. sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna; dan l. kata laluan hendaklah ditukar apabila disyaki berlakunya kebocoran kata laluan atau dikompromi.	
PKSMOT-K05/03 Capaian Sistem Pengoperasian		
PKSMOT-K05/03/01 Capaian Sistem Pengoperasian		
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu 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; b. merekodkan capaian yang berjaya dan gagal; dan c. membekalkan kemudahan untuk pengesahan (bagi sistem kata laluan kunci digunakan, kualiti kata kunci perlu mendapat pengesahan). Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a. mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; b. mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan c. menjana amaran (*alert*) sekiranya berlaku	Pentadbir Sistem

	pelanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi termasuk berikut: a. mengawal capaian ke atas sistem operasi menggunakan kaedah *log on* yang terjamin; b. mewujudkan satu pengenalan diri (*ID*) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna; c. mewujudkan fungsi pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah kukuh mengikut polisi kata laluan yang berkuat kuasa; dan d. mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
PKSMOT-K05/04	**Capaian Aplikasi dan Maklumat**	
	Bertujuan melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di MOT adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: a. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (*log*) bagi mengesan aktiviti-aktiviti yang tidak diingini;	Pentadbir Sistem

	c. memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; e. capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; f. maklumat tarikh *login* terakhir hendaklah direkodkan; dan g. digalakkan *session timeout* dilaksanakan.	
PKSMOT-K05/05	**Capaian Jarak Jauh**	
	a. Capaian jarak jauh yang dimaksudkan merangkumi: i. capaian daripada sistem rangkaian dalaman;dan ii. capaian daripada sistem rangkaian b. penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah penyulitan (*encryption*); c. lokasi bagi akses ke sistem ICT MOT hendaklah dipastikan selamat; dan d. penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pengurus ICT/ICTSO. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Pentadbir Sistem, Pengguna

	e. Capaian jarak jauh boleh juga menggunakan VPN yang dilaksanakan hanya untuk capaian ke sistem tertentu dalam masa yang ditetapkan seperti di dalam Garis Panduan Penggunaan Capaian *Virtual Private Network* (VPN) dan Aplikasi Sidang Video di Kementerian Pengangkutan Malaysia; f. Sekiranya pengguna MOT memerlukan akses bagi kemudahan tersebut, mohon untuk mendapatkan akses dan kebenaran dan tertakluk kepada syarat di bawah : ● Mendapat kebenaran daripada Pengurus ICT atau ICTSO. ● Ruang kerja dan persekitaran bagi akses ke sistem MOT hendaklah dipastikan selamat. g. Sekiranya Pihak Luaran memerlukan akses dan kemudahan tersebut, Pihak Luaran tersebut perlu memohon untuk mendapat kebenaran daripada Pengurus ICT atau ICTSO. n luaran ke sistem rangkaian dalaman. h. Permohonan untuk mendapatkan akses dan kebenaran tertakluk kepada syarat di bawah : ● Ruang kerja dan persekitaran bagi akses ke sistem MOT hendaklah dipastikan selamat; ● Tujuan penggunaan yang jelas seperti penyelenggaraan, troubleshoot dan lain-lain yang berkaitan; ● Tempoh capaian yang telah ditetapkan bergantung kepada tujuan penggunaan; i. Peralatan yang digunakan hendaklah mempunyai perisian antivirus dan perisian keselamatan seumpamanya yang sentiasa dikemaskini.	

PKSMOT-K05/06 Kawalan Capaian Rangkaian		
PKSMOT-K05/06/01 Capaian Rangkaian		
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian MOT dan rangkaian awam; b. mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya; c. memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; d. capaian pengguna jarak jauh (*remote user*) perlulah dikawal dan dipantau; e. capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal berpandukan Prosedur Pengurusan Konfigurasi; f. penggunaan Internet di MOT hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian dan Keselamatan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MOT; g. penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; dan h. *Content Filtering* atau peralatan keselamatan yang lain boleh digunakan untuk mengawal dan memantau akses ke Internet. Pengecualian akan dipertimbangkan bagi setiap permohonan.	Pentadbir Rangkaian dan Keselamatan

PKSMOT-K05/06/02 Capaian Internet		
	a. penggunaan Internet di MOT hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian dan Keselamatan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MOT; b. penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; dan c. *Content Filtering* atau peralatan keselamatan yang lain boleh digunakan untuk mengawal dan memantau akses ke Internet. Pengecualian akan dipertimbangkan bagi setiap permohonan.	Pentadbir Rangkaian dan Keselamatan Pengurus ICT
PKSMOT-K05/07 Peralatan Mudah Alih		
	Perkara yang perlu dipatuhi adalah seperti berikut: a. merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kehilangan atau kerosakan; b. peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan; dan c. memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.	Pegawai Aset ICT, Pengguna
PKSMOT-K05/08 *Bring Your Own Device* (BYOD)		
	BYOD merupakan peralatan mudah alih persendirian seperti telefon pintar, komputer tablet atau komputer riba yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian MOT.	Pengguna

	Pengguna yang menggunakan kemudahan rangkaian MOT dan MyGovNet/PCN atau data line persendirian untuk akses perisian dan aplikasi dalaman MOT tertakluk kepada PKS MOT dan pekeliling berkaitan yang sedang berkuat kuasa. Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut : a. mengelak risiko kebocoran maklumat rasmi; b. mengelakkan ancaman risiko keselamatan ICT; c. memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi jabatan; dan d. meningkatkan integriti data. Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD. Bagi mengawal dan memantau pelaksanaan BYOD, mekanisme kawalan diwujudkan seperti berikut: a. mengaktifkan fungsi keselamatan kata laluan bagi mengelakkan akses yang tidak dibenarkan. b. Pastikan peralatan BYOD bebas daripada sebarang malware dan ancaman keselamatan. c. Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.	
PKSMOT-K05/09 Telekerja		
	Telekerja merujuk kepada pekerjaan yang dijalankan secara jarak jauh untuk melaksanakan tugas rasmi melalui aplikasi telesidang dan aplikasi perhubungan	

	sosial tertakluk kepada PKS MOT yang sedang berkuat kuasa. Penggunaan Aplikasi Mesyuarat Jarak Jauh seperti *Microsoft Teams, Google Meet, Zoom, Cisco Webex* dan lain-lain perisian hendaklah dipastikan tahap integriti dan keselamatan aplikasi terjamin. Penggunaan Aplikasi Perhubungan Sosial hendaklah menggunakan aplikasi yang mempunyai fungsi *End-To-End* Encryption (E2EE) serta tahap integriti dan keselamatan aplikasi terjamin. Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan semasa telekerja seperti berikut : a. mengelak risiko kebocoran maklumat rasmi; b. mengelakkan ancaman risiko keselamatan ICT; c. memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi jabatan; dan d. meningkatkan integriti data. e. Segala dokumen terperingkat adalah dilarang untuk dihantar melalui telekerja melainkan dokumen tersebut di encryption terlebih dahulu. Bagi mengawal dan memantau pelaksanaan telekerja, mekanisme kawalan diwujudkan seperti berikut: a. mengaktifkan fungsi *Virtual Private Network* (VPN) bagi akses kepada rangkaian jabatan yang terkawal; dan b. mengaktifkan fungsi keselamatan kata laluan dan encryption bagi mengelakkan akses yang tidak dibenarkan.	

	Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada persekitaran telekerja.	
PKSMOT-K05/10 Pengkomputeran Awan (*Cloud Computing*)		
	Pengkomputeran Awan adalah perkhidmatan sumber-sumber ICT yang dimayakan tanpa penyediaan infrastruktur di pihak pengguna. Penggunaan dan penyediaan perkhidmatan pengkomputeran awan perlu mendapat kelulusan daripada pihak bertanggungjawab. Pengkomputeran awan hendaklah dipastikan selamat bagi menjamin keselamatan maklumat berdasarkan penerangan berikut : i. Pengkomputeran Awan adalah perkhidmatan sumber-sumber ICT yang dimayakan tanpa penyediaan infrastruktur di pihak pengguna; ii. Penggunaan dan penyediaan perkhidmatan pengkomputeran awan perlu mendapat kelulusan daripada pihak kerajaan; iii. Pengkomputeran awan hendaklah dipastikan selamat bagi menjamin keselamatan maklumat; dan Penggunaan Teknologi Pengkomputeran Awan adalah tertakluk kepada peraturan, pekeliling dan dasar Perkhidmatan Pengkomputeran Awan Sektor Awam yang berkuat kuasa.	Pentadbir Sistem, Pengguna

KAWALAN 06 : KAWALAN KRIPTOGRAFI

PKSMOT - K06 **Objektif**		
Melindungi kerahsiaan, integriti dan kesahihan maklumat yang merangkumi data dalam sistem rangkaian, sistem aplikasi dan pangkalan data.		
PKSMOT-K06/01 Kriptografi		
	Melindungi kerahsiaan, integriti dan kesahihan maklumat yang merangkumi data di dalam sistem rangkaian, sistem aplikasi dan pangkalan data. Kunci penyulitan mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. Kriptografi turut merangkumi kaedah-kaedah seperti berikut: a. Kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan dan dibuat penyulitan; dan b. Penggunaan PKI (*Public Key Infrastructure*) yang selamat yang dibekalkan oleh Kerajaan.	Pentadbir Sistem, Pengguna
PKSMOT-K06/01/01 Penyulitan		
	Pengguna hendaklah menggunakan penyulitan (encryption) ke atas maklumat sensitif atau maklumat terperingkat melalui kaedah penyulitan yang sesuai pada setiap masa. Penghantaran dokumen, maklumat atau e-mel terperingkat hendaklah menggunakan penyulitan (encryption) ke atas fail, maklumat atau e-mel tersebut berdasarkan pekeliling berkuatkuasa.	Pentadbir Sistem, Pengguna

PKSMOT-K06/01/02 Tandatangan Digital		
	Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. penggunaan token atau sijil digital hendaklah digunakan bagi capaian sistem yang dikhususkan; b. token hendaklah disimpan dengan selamat bagi mengelakkan sebarang kecurian atau disalah guna oleh pihak ketiga; c. perkongsian penggunaan token adalah tidak dibenarkan sama sekali; dan d. sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pengeluar token.	Pengguna
PKSMOT-K06/01/03 Pengurusan Infrastruktur Kunci Awam (PKI)		
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut. Tindakan berikut perlu dipatuhi. a. Semua sistem aplikasi yang boleh diakses oleh umum dan mempunyai transaksi login, bayaran atau sebarang maklumat sensitif hendaklah dipasang dengan Sijil SSL daripada pembekal yang diiktiraf oleh kerajaan; dan b. Perisian yang digunakan untuk menjana, menyimpan dan mengarkib kunci penyulitan perlu dilindungi secara fizikal.	Pentadbir Sistem, Pengguna

KAWALAN 07 : KESELAMATAN FIZIKAL & PERSEKITARAN

PKSMOT - K07 Objektif		
Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.		
PKSMOT-K07/01 Keselamatan Kawasan		
PKSMOT-K07/01/01 Kawasan Larangan ICT		
	Kawasan larangan ICT bagi MOT ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga MOT yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis tersebut. Kawasan larangan lokasi ICT MOT adalah Pusat Data MOT. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut: a. sumber data atau *server,* peralatan komunikasi dan storan perlu ditempatkan di pusat data yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran; b. akses adalah terhad kepada warga MOT yang telah diberi kuasa sahaja dan dipantau pada setiap masa; c. pemantauan dilaksanakan menggunakan peralatan yang bersesuaian seperti CCTV; d. peralatan keselamatan fizikal seperti CCTV dan sistem akses masuk perlu diperiksa secara berkala; e. butiran pelawat yang keluar masuk ke Pusat Data hendaklah direkodkan; f. pelawat yang masuk ke Pusat Data perlu sentiasa diawasi atau diiringi sepanjang masa mengikut keperluan sewajarnya; g. lokasi Pusat Data hendaklah tidak berhampiran dengan kawasan laluan awam;	Pentadbir Pusat Data

	h. memperkukuhkan dinding, siling, tingkap dan pintu termasuk memastikan pintu sentiasa dikunci untuk mengawal kemasukan dan mengelakkan pecah masuk; dan i. mengehadkan jalan keluar masuk.	
PKSMOT-K07/01/02 Kawalan Masuk Fizikal		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Warga MOT i. semua warga hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; dan ii. semua pas keselamatan hendaklah diserahkan kembali kepada MOT apabila pengguna berhenti atau bersara. b. Pelawat i. setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu masuk utama Premis MOT. Pas ini hendaklah dikembalikan semula selepas tamat lawatan. c. Kehilangan Pas Kehilangan pas mestilah dilaporkan dengan segera.	Pengguna / Pelawat
PKSMOT-K07/02 Keselamatan Peralatan		
PKSMOT-K07/02/01 Peralatan ICT		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;	Pengguna, Pentadbir Sistem, Pegawai Aset ICT

	b. pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; d. pengguna mesti memastikan perisian *antivirus* bagi semua peralatan ICT yang dibekalkan oleh Jabatan seperti komputer peribadi, *notebook, server* dan lain- lain yang berada di bawah tanggungjawab mereka sentiasa aktif *(activated)* dan dikemas kini di samping turut melakukan imbasan ke atas media storan yang digunakan; e. semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; f. aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang bertanggungjawab. Arahan Keselamatan Kerajaan hendaklah sentiasa dipatuhi bagi mengelak berlakunya kerosakan atau kehilangan aset; g. sekiranya peralatan ICT tidak digunakan, peralatan tersebut hendaklah disimpan di dalam almari atau kabinet atau peti besi atau stor atau bilik khas yang berkunci untuk penyimpanan peralatan ICT; h. peralatan ICT yang kritikal perlu disokong oleh UPS; i. UPS yang berkuasa tinggi perlu diletakkan di bilik yang berasingan bersuhu rendah yang dilengkapi dengan pengudaraan yang sesuai;	

	j. semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switch, router* dan lain-lain perlu diletakkan di dalam bilik atau rak berkunci; k. semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai; l. peralatan ICT yang hendak dibawa keluar dari premis MOT, perlulah mendapat kelulusan Pegawai Aset ICT; dan m. aset ICT yang hilang hendaklah dilaporkan mengikut pekeliling perbendaharaan sedia ada.	
PKSMOT-K07/02/02	***Clear Desk* dan *Clear Screen***	
	Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: *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 daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Pengguna

PKSMOT-K07/02/03	**Media Tandatangan Digital**	
	Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut: a. pengguna hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. tidak boleh dipindah milik atau dipinjamkan; dan c. sebarang kehilangan yang berlaku hendaklah dilaporkan kepada pihak yang dipertanggungjawabkan.	Pentadbir Sistem, Pengguna
PKSMOT-K07/02/04	**Perisian Dan Aplikasi**	
	Sebarang perisian dan aplikasi yang digunakan hendaklah mematuhi langkah–langkah berikut: a. hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan jabatan; b. lesen perisian *(registration code, serials, CD-keys)* perlu disimpan berasingan daripada *CD-ROM*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; c. kod sumber *(source code)* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan; dan d. sistem aplikasi, perisian dan kod sumber tidak dibenarkan dikongsi, diagih, dibawa keluar atau didemonstrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT.	Pengurus ICT, Pegawai Aset ICT, Pentadbir Sistem

PKSMOT-K07/02/05	**Perkakasan Tanpa Penyeliaan *(Unattended Equipment)***	
	Pengguna perlu memastikan mana-mana perkakasan yang ditinggalkan tanpa penyeliaan mematuhi ciri-ciri keselamatan seperti mempunyai kata laluan dan sebagainya. Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.	Pengguna
PKSMOT-K07/02/06	**Peralatan di Luar Premis**	
	Peralatan ICT yang dibawa keluar dari premis MOT adalah terdedah kepada pelbagai risiko. Peralatan ICT yang hendak dibawa keluar perlu mengisi Borang Permohonan Kebenaran Membawa Aset Alih ICT Kerajaan Ke Luar Pejabat Kementerian Pengangkutan Malaysia (BPM-OKI-B3.1) atau Borang Permohonan Pergerakan/ Pinjaman Peralatan ICT Sewaan (BPM-OKI-B4.0) yang boleh dicapai di Sistem Intranet MOT. Peralatan ICT yang dibawa keluar premis MOT merangkumi: a. penggunaan perkakasan secara sementara bagi keperluan mesyuarat, latihan dan sebagainya; dan b. penempatan perkakasan secara kekal di sesebuah agensi lain. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pentadbir Sistem

PKSMOT- K07/02/07 Pelupusan		
	Aset ICT yang hendak dilupuskan perlu mematuhi tatacara pelupusan semasa. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT MOT dilupuskan dengan teratur iaitu: a. pegawai aset ICT akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; b. peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaska*n*; c. data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; d. pelupusan peralatan ICT boleh dilakukan secara berpusat atau tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa; e. sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan; f. maklumat lanjut berhubung pelupusan boleh dirujuk kepada pekeliling perbendaharaan semasa yang berkuat kuasa; dan g. pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara.	Pegawai Aset ICT, Pengguna
PKSMOT-K07/02/08 Penyelenggaraan		
	Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:	Pentadbir Sistem, Pegawai Aset ICT

	a. mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang di selenggara; b. memastikan perkakasan hanya diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan d. memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
PKSMOT-K07/03 Kawalan Persekitaran		
PKSMOT-K07/03/01 Kawalan Persekitaran		
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu ke Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a. merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. semua ruang pejabat khususnya yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;	Pengurus ICT

	e. semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g. semua peralatan perlindungan keselamatan dan kebakaran hendaklah diselenggara bagi memastikan ia dapat berfungsi dengan baik.	
PKSMOT-K07/03/02 Kabel Rangkaian		
	a. semua kabel perlu dilabel dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; b. menggunakan kabel mengikut spesifikasi yang telah ditetapkan; dan c. melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping.*	Pentadbir Rangkaian
PKSMOT-K07/03/03 Bekalan Kuasa		
	Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: a. semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. peralatan sokongan seperti UPS dan penjana kuasa *(power generator)* boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan c. semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Pengurus ICT

PKSMOT-K07/03/04 Prosedur Kecemasan		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Pelan Tindakan dan Kecemasan MOT; dan b. kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Kebakaran yang dilantik mengikut aras.	Pengguna, Pegawai Keselamatan Kebakaran
PKSMOT-K07/03/05 Mekanisme Pelaporan Insiden Bukan ICT		
	Semua pengguna yang terlibat haruslah melaporkan dan merekodkan sebarang kejadian atau kerosakan peralatan bukan ICT kepada pihak Bahagian Pentadbiran.	Pengguna
PKSMOT-K07/03/06 Mekanisme Kawalan Peralatan Sewaan/Uji Coba *(Proof Of Concept)*		
	a. Penerimaan i. peralatan yang diterima bebas daripada virus, *backdoor, worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT jabatan. b. Penyelenggaraan i. capaian melalui rangkaian luar MOT adalah tidak dibenarkan kecuali mendapat kebenaran bertulis ICTSO; dan ii. aktiviti penyelenggaraan adalah di bawah pengawasan pegawai MOT. c. Pemulangan i. maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal *(secured delete)*; dan ii. memastikan semua maklumat jabatan tidak tertinggal pada peralatan.	Pentadbir Sistem

PKSMOT-K07/04 Keselamatan Sistem Dokumentasi		
	Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: a. memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada; c. setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; d. pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; e. kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; dan f. menggunakan penyulitan *(encryption)* ke atas dokumen rahsia rasmi yang disediakan, disimpan dan dihantar secara elektronik.	Pentadbir Sistem, Pentadbir Fail

KAWALAN 08 : KESELAMATAN OPERASI

PKSMOT-K08 **Objektif**		
Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.		
PKSMOT-K08/01 Prosedur Operasi		
PKSMOT-K08/01/01 Pengendalian Dokumen Prosedur Operasi		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. semua prosedur operasi ICT yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b. setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap; dan c. semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pentadbir Sistem
PKSMOT-K08/01/02 Pengurusan Perubahan		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. pengubahsuaian melibatkan perkakasan, sistem pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran Pengurus ICT, pegawai atasan atau pemilik aset ICT terlebih dahulu; b. aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Pentadbir Sistem

	c. semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau sebaliknya.	
PKSMOT-K08/01/03 Pengasingan Tugas dan Tanggungjawab		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. tugas mewujud, memadam, mengemaskini , mengubah dan mengesahkan data hendaklah dilakukan oleh pegawai yang berlainan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c. perkakasan dan rangkaian yang digunakan bagi pembangunan dan penyelenggaraan aplikasi hendaklah diasingkan daripada persekitaran produksi.	Pengurus ICT, Pentadbir Sistem

PKSMOT-K08/02 Perancangan dan Penerimaan Sistem		
PKSMOT-K08/02/01 Perancangan Kapasiti		
	Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti olel pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem
PKSMOT-K08/02/02 Penerimaan Sistem		
	Semua sistem baharu (termasuk sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem
PKSMOT-K08/03 Perlindungan dari Perisian Berbahaya		
PKSMOT-K08/03/01 Perlindungan dari Perisian Berbahaya		
	Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya: a. memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus atau endpoint keselamatan, *Intrusion Prevention System* (IPS), *e-mel filtering*, firewall, *content filtering* dan lain-lain perkakasan atau sistem keselamatan yang berkaitan mengikut prosedur penggunaan yang betul dan selamat; b. memasang dan menggunakan hanya perisian yang tulen; c. mengimbas semua perisian, sistem, media storan dan kepilan fail dengan *antivirus* yang telah disediakan oleh Jabatan sebelum menggunakannya;	Pentadbir Sistem, Pengguna

	d. memastikan paten *antivirus* atau agen *endpoint* keselamatan pada peralatan atau perisian ICT dikemaskini dengan versi terkini; e. menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; dan f. memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya.	
PKSMOT-K08/03/02 Perlindungan dari *Mobile Code*		
	Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pengguna
PKSMOT-K08/04 *Housekeeping*		
PKSMOT-K08/04/01 *Backup*		
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana atau insiden, *backup* seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. *Backup* hendaklah direkodkan dan disimpan di *off site*, di antaranya adalah: a. membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu; b. membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi; c. menguji sistem *backup* sedia ada dan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan d. *backup* dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.	Pentadbir Sistem

	e. Prosedur *backup* boleh dirujuk pada dokumen Prosedur Pengoperasian Pengurusan Pusat Data.	
PKSMOT-K08/05 Pengurusan Media		
PKSMOT-K08/05/01 Media Storan Mudah Alih		
	Penghantaran atau pemindahan media storan mudah alih yang mengandungi maklumat terperingkat ke luar pejabat mestilah mematuhi pekeliling yang terkini dan berkuat kuasa.	Pengguna
PKSMOT-K08/05/02 Prosedur Pengendalian Media		
	Di antara prosedur-prosedur pengendalian media termasuk: a. melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. meng hadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan e. media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut peraturan dan prosedur yang betul dan selamat.	Pentadbir Sistem, Pengguna
PKSMOT-K08/06 Paparan Maklumat Umum		
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat umum adalah seperti berikut: a. memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; b. memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan sebelum dimuat naik ke portal; dan	Pengguna

	c. memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian.	
PKSMOT-K08/07 Pemantauan		
PKSMOT-K 08/07/01 Pemantauan		
	Bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut: a. *log audit* yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang difikirkan sesuai dan boleh diterima bagi memantau kawalan capaian; b. prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala; c. kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. kesalahan, kesilapan atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya; dan e. masa yang berkaitan dengan sistem pemprosesan maklumat dalam MOT perlu diselaraskan dengan sumber masa yang dipersetujui.	Pentadbir Sistem
PKSMOT-K08/07/02 Pengauditan dan Forensik ICT		
	CSIRT MOT mestilah bertanggungjawab merekod dan menganalisis: a. sebarang percubaan pencerobohan kepada sistem ICT MOT; b. serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery*), pencerobohan (*intrusion*) ancaman (*threats*) dan kehilangan fizikal (*physical loss*);	CSIRT MOT, ICTSO Pentadbir Sistem

	c. pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e. aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian; g. aktiviti penyalahgunaan akaun e-mel; dan h. aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian. Langkah-langkah yang perlu diambil adalah seperti berikut: a. CSIRT MOT akan menentukan prosedur pengumpulan bahan bukti yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan; b. proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; c. sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan; dan d. semua proses dan hasil siasatan adalah **SULIT**.	

PKSMOT-K08/07/03 Jejak Audit		
	Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi ciri-ciri berikut: a. rekod setiap aktiviti transaksi; b. maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c. aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d. maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir Sistem hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem
PKSMOT-K08/07/04 Sistem Log		
	Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya enam (6) bulan. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti berikut: i. Fail log sistem pengoperasian; ii. Fail log servis (web, e-mel); iii. Fail log aplikasi *(audit trail)*; dan iv. Fail log rangkaian *(switch, firewall, IPS)*	Pentadbir Sistem

	Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a. mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	
PKSMOT-K08/07/05	**Penyeragaman Jam (*Clock Synchronization*)**	
	Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MOT atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan iaitu my.pool.ntp.org.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT MOT

KAWALAN 09 : KESELAMATAN KOMUNIKASI

PKSMOT-K09 **Objektif**		
Memastikan sistem komunikasi yang digunakan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
PKSMOT-K09/01 Pengurusan Rangkaian		
	Infrastruktur Rangkaian perlu dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: a. semua tanggungjawab atau kerja-kerja operasi dan rangkaian hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; c. semua capaian kepada Internet dan sistem aplikasi mestilah melalui *firewall*; d. memasang perisian IPS bagi mengesan dan menghalang sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem danmaklumat MOT; e. menggunakan *Web Content Filter* untuk menyekat aktiviti yang dilarang; f. memasang sistem penapis e-mail (*E-mail filtering/ Antispam*) untuk menapis sistem e-mail MOT; g. semua aplikasi MOT yang boleh diakses daripada luar (*public)* hendaklah melalui *Web Application Firewall* (WAF) atau perisian lain yang mempunya fungsi setaranya;	Pentadbir Rangkaian

	h. pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian; i. sebarang penyambungan rangkaian yang bukan di bawah kawalan MOT adalah tidak dibenarkan kecuali dengan kebenaran khas Pengurus ICT atau ICTSO; dan j. kemudahan bagi *wireles* hendaklah dilengkapi dengan kawalan keselamatan.	
PKSMOT-K09/02 Pengurusan Penghantaran dan Penerimaan Maklumat		
	Bertujuan untuk memastikan keselamatan penghantaran dan penerimaan maklumat dan perisian dalam agensi dan mana-mana entiti luar terjamin. a. polisi, prosedur dan kawalan penghantaran dan penerimaan maklumat yang formal perlu diwujudkan untuk melindungi maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. perjanjian perlu diwujudkan untuk penghantaran dan penerimaan maklumat dan perisian di antara MOT dengan pihak luar; c. media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan dan penerimaan; d. maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan e. maklumat lanjut berkenaan perkongsian data merentas agensi boleh dirujuk kepada pekeliling semasa yang berkuatkuasa.	Pentadbir Sistem
PKSMOT-K09/03 Pengurusan Mel Elektronik (E-mel)		
	Penggunaan e-mel di MOT/Jabatan hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan tatacara penggunaan e-mel dan Internet yang terkandung dalam **Tatacara Penggunaan E-Mel Dan Internet MOT dan Prosedur Pengurusan E-mel dan**	Pentadbir E-mel, Pegawai Tadbir Bahagian

	Akaun Pengguna yang boleh dicapai di Sistem Intranet MOT. Penghantaran e-mail terperingkat melalui e-mail hendaklah menggunakan penyulitan dengan menggunakan algorithm yang diiktiraf oleh *National Trusted Cryptographic Algorithm List* (MySEAL).	
PKSMOT-K09/04 Pengurusan Penggunaan Sidang Video *(Video Conferencing)*		
	Penggunaan Sidang Video di MOT hendaklah mematuhi **Garis Panduan Penggunaan Capaian VPN Dan Komunikasi Sidang Video MOT** untuk memastikan Sidang Video dapat dijalankan dengan lancar. Garis panduan boleh dicapai melalui Sistem Intranet MOT untuk rujukan.	Pentadbir Sistem
PKSMOT-K09/05 Keselamatan Perkhidmatan Rangkaian		
	Pengurusan bagi semua perkhidmatan rangkaian (*in-house atau out-source*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti. Mekanisme keselamatan dan tahap perkhidmatan hendaklah dimasukkan di dalam perjanjian perkhidmatan rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Komponen keselamatan rangkaian merangkumi perkakasan, perisian dan perkhidmatan perkomputeran awan digunakan bagi memastikan rangkaian selamat dari ancaman, serangan siber, cubaan pengodaman dan kecuaian Pengguna; b. Sistem Keselamatan Rangkaian menggunakan kombinasi pelbagai komponen keselamatan rangkaian bagi	ICTSO, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT, Pentadbir Sistem ICT MOT, Pembekal dan Pihak Ketiga

	membentuk sistem pertahanan berlapis(layered defense system); dan c. Setiap lapisan sistem pertahanan membekal keupayaan pemantauan, pengenalan dan pemulihan bagi memastikan rangkaian selamat.	
PKSMOT-K09/06 Pengasingan Dalam Rangkaian		
	Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian MOT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengenal pasti fungsi dan tanggungjawab pengguna; b. Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Mengemaskinikan hak capaian pengguna dari semasa ke semasa mengikut keperluan; dan e. Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT dan Pentadbir Sistem ICT MOT

PKSMOT-K09/07	**Pemindahan/ Pertukaran Data dan Maklumat**	
PKSMOT-K09/07/01	**Polisi dan Prosedur Pemindahan/ Pertukaran Data dan Maklumat**	
	MOT perlu mengambil kira keselamatan maklumat apabila berlaku pemindahan data dan maklumat organisasi antara MOT dengan pihak luar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mewujudkan polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; b. Menyediakan perjanjian atau kebenaran bertulis untuk pertukaran maklumat dan perisian di antara MOT dengan pihak agensi luar; c. Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, didedahkan, disalah guna atau dirosakkan semasa pemindahan keluar dari MOT; dan d. Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya.	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data Rangkaian dan Komunikasi ICT MOT dan Pengguna
PKSMOT-K09/07/02	**Perjanjian Mengenai Pemindahan/Pertukaran Data dan Maklumat**	
	MOT perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan/pertukaran data dan maklumat organisasi antara MOT dengan pihak luar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal penghantaran dan penerimaan maklumat;	Pemilik Sistem dan PICT MOT

	b. Memastikan prosedur keupayaan mengesan dan tanpa sangkalan semasa pemindahan/pertukaran data dan maklumat; c. Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan/pertukaran data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan d. Mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	
PKSMOT-K09/08 Perjanjian Kerahsiaan atau Ketakdedahan		
	Syarat-syarat perjanjian kerahsiaan atau non-disclosure perlu mengambil kira keperluan MOT dan hendaklah disemak dan didokumentasikan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah memahami dan menandatangani perjanjian kerahsiaan Akta Rahsia Rasmi 1972 (Akta 88) seperti yang terkandung di dalam Arahan Keselamatan Kerajaan yang sedang berkuatkuasa. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan; dan b. Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.	ICTSO, Pentadbir Sistem ICT MOT, Pembekal dan Pengguna

KAWALAN 10 : PEROLEHAN, PEMBANGUNAN & PENYELENGGARAAN SISTEM

PKSMOT-K10	**Objektif**	
Memastikan sistem yang dibangunkan sendiri secara dalaman atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
PKSMOT-K10/01	**Kawalan Proses Aplikasi**	
	a. perolehan dan pembangunan, penambahbaikan serta penyelenggaraan sistem secara dalaman atau luaran hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu sistem pemprosesan dan ketepatan maklumat; b. ujian keselamatan hendaklah dijalankan ke atas sistem aplikasi untuk menyemak pengesahan dan integriti data; dan c. sistem yang dibangunkan atau digunakan hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan sebelum digunakan.	Pentadbir Sistem, ICTSO
PKSMOT-K10/01/01	**Pengesahan Data *Input***	
	Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pentadbir Sistem
PKSMOT-K10/01/02	**Kawalan Proses**	
	Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem
PKSMOT-K10/01/03	**Pengesahan Data *Output***	
	Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem

PKSMOT-K10/02 Keselamatan Fail Sistem		
	Fail sistem perlu dikawal dan dikendalikan dengan baik dan selamat. a. proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d. mengaktifkan log audit bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; dan e. data ujian hendaklah dipilih dan penggunaannya dikawal serta dilindungi.	Pentadbir Sistem
PKSMOT-K10/03 Keselamatan Dalam Proses Pembangunan dan Sokongan		
PKSMOT-K10/03/01 Peraturan Keselamatan Dalam Pembangunan Sistem		
	Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi.	Pengurus ICT
PKSMOT-K10/03/02 Prosedur Perubahan		
	Perubahan atau pengubahsuaian ke atas kitaran hayat pembangunan sistem, sistem pengoperasian dan aplikasi hendaklah dikawal, diuji, di rekod dan disahkan sebelum digunakan mengikut SOP yang telah ditetapkan.	Pentadbir Sistem dan Pemilik Proses atau Sistem

PKSMOT-K10/03/03 Semakan Teknikal Aplikasi Selepas Perubahan Platform		
	Semakan dan pengujian terhadap aplikasi perlu dilaksanakan sekiranya berlaku perubahan terhadap platform pengoperasian bagi memastikan fungsi dan operasi sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan sistem aplikasi, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan; dan b. Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan.	Pentadbir Sistem
PKSMOT-K10/03/04 Kawalan Terhadap Perubahan Kepada Perisian		
	Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.	Pentadbir Sistem
PKSMOT-K10/03/05 Prinsip Kejuruteraan Sistem Yang Selamat		
	Prinsip kejuruteraan sistem yang selamat hendaklah dibangunkan, didokumenkan, dikaji dan diguna pakai ke atas semua pelaksanaan sistem maklumat.	Pentadbir Sistem
PKSMOT-K10/03/06 Persekitaran Pembangunan Sistem Yang Selamat		
	Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem.	Pentadbir Sistem
PKSMOT-K10/03/07 Pembangunan Sistem Secara Luaran *(Outsource)*		
	Pembangunan perisian aplikasi secara *outsource* hendaklah mematuhi perkara-perkara berikut: a. setiap projek perlu dipantau oleh Pengurus ICT; b. kontrak perbekalan hendaklah memasukkan klausa kod sumber menjadi hak milik MOT;	Pengurus ICT

	c. kod sumber yang diserahkan kepada MOT mesti bebas daripada sebarang ralat dan kerentanan; d. mengutamakan kepakaran teknologi tempatan; e. pembangunan aplikasi hendaklah dijalankan dalam persekitaran pengkomputeran MOT; f. penggunaan *data masking* semasa pengujian; g. data ujian hendaklah dilupuskan secara kekal *(secured delete)* selepas projek disiapkan/tamat kontrak; dan h. aktiviti *backup* hendaklah berjaya dilakukan sebelum projek tamat.	
PKSMOT-K10/03/08 Ujian Keselamatan Sistem		
	Aktiviti pengujian keselamatan sistem hendaklah dilaksanakan atas sistem baharu, tambah baik, naik taraf dan versi baharu berdasarkan kriteria yang telah ditetapkan.	Pengurus ICT, Pentadbir Sistem
PKSMOT-K10/03/09 Pembocoran Maklumat		
	Sebarang peluang untuk membocorkan maklumat perlu dilarang dan dihalang.	ICTSO
PKSMOT-K10/04 Data Ujian		
	Memastikan data yang digunakan untuk pengujian adalah dilindungi.	Pengurus ICT
PKSMOT-K10/05 Kawalan Terhadap Keterdedahan Teknikal		
	Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. memperoleh maklumat keterdedahan teknikal sistem maklumat yang digunakan; b. menilai tahap kerentanan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan	Pentadbir Sistem, ICTSO

	c. mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	
PKSMOT-K10/06 Perkhidmatan E-dagang		
	Bertujuan untuk memastikan keselamatan perkhidmatan e- dagang dan penggunaannya. a. maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b. maklumat yang terlibat dalam transaksi dalam talian *(on-line)* perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c. integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Pentadbir Sistem, Pengguna
PKSMOT-K10/07 Pembangunan Aplikasi Mudah Alih		
	Menerangkan perkara yang perlu dipatuhi dalam membangunkan aplikasi mudah alih agar lebih selamat.	Pentadbir Sistem
PKSMOT-K10/07/01 Prosedur Integrasi Pembangunan Aplikasi Mudah Alih		
	Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	Pentadbir Sistem

KAWALAN 11 : HUBUNGAN PEMBEKAL

PKSMOT-K11 **Objektif**		
Memastikan aset ICT MOT yang boleh dicapai oleh pembekal dilindungi. Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa.		
PKSMOT-K11/01 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal		
	Perkara–perkara yang perlu dipatuhi adalah seperti berikut: a. pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas; b. pengurusan pembekal adalah tertakluk kepada peraturan yang sedang berkuat kuasa; c. pengawalan dan pemantauan akses pembekal; d. keperluan minimum keselamatan maklumat bagi setiap pembekal seperti keperluan perundangan atau pekeliling berkaitan hendaklah dinyatakan dalam perjanjian; e. memastikan semua pembekal menandatangani Surat Akuan Pematuhan PKS MOT seperti di **Lampiran 1** dan Perakuan Akta Rahsia Rasmi 1972 [Akta 88] seperti di **Lampiran 2**; f. Akses kepada aset ICT MOT perlu berlandaskan kepada perjanjian kontrak perkhidmatan yang telah dipersetujui dengan pihak ketiga; g. Capaian dari luar rangkaian MOT oleh pihak ketiga adalah **TIDAK DIBENARKAN** kecuali dengan kebenaran ICTSO melalui Pentadbir Sistem; dan h. Capaian kepada kod sumber program dari luar pejabat oleh pihak ketiga **TIDAK DIBENARKAN**	Pengurus ICT, Pentadbir Sistem, Pembekal

	kecuali mendapat kebenaran bertulis ICTSO melalui Pentadbir Sistem. Semua perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut peraturan-peraturan semasa. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. perubahan dalam perjanjian dengan pembekal; b. perubahan yang dilakukan oleh MOT bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian polisi dan prosedur; dan c. perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	
PKSMOT-K11/02 Pengurusan Penyampaian Perkhidmatan Pembekal		
	Keselamatan Maklumat yang dipersetujui dalam perjanjian bersama pembekal perlu dipatuhi untuk mengekalkan tahap keselamatan maklumat. MOT hendaklah sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal melalui jawatankuasa pemantauan yang ditubuhkan. Perkara-perkara berikut hendaklah dipatuhi: a. pemantauan tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan; dan b. laporan perkhidmatan yang dihasilkan oleh pembekal hendaklah dipantau dan status kemajuan dikemukakan kepada MOT.	Pengurus ICT, Pentadbir Sistem

	Semua perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut peraturan-peraturan semasa. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. perubahan dalam perjanjian dengan pembekal; b. perubahan yang dilakukan oleh MOT bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian polisi dan prosedur; dan c. perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	
PKSMOT-K11/03 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal		
	Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap Pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat MOT. Pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak MOT selaras dengan peraturan dan kawalan keselamatan yang sedang berkuat kuasa. Sekiranya Pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang Pembekal daripada melaksanakan perkhidmatan tersebut.	Pembekal

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. MOT hendaklah memilih pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b. Semua wakil Pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; c. Produk atau perkhidmatan yang ditawarkan oleh Pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; d. Penilaian teknikal oleh Jawatankuasa Penilaian Teknikal boleh dilaksanakan melalui laporan yang dikemukakan oleh Pembekal; e. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan MOT; dan f. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh MOT.	
PKSMOT-K11/04 Kawalan Keselamatan Maklumat Bagi Rantaian Bekalan ICT		
	Perjanjian dengan pembekal utama hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau	Pemilik Sistem, PICT dan Pembekal

	pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan c. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	
PKSMOT-K11/05 Memantau dan Mengkaji Semula Perkhidmatan Pembekal		
	MOT hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memantau tahap prestasi perkhidmatan untuk mengesahkan Pembekal mematuhi perjanjian perkhidmatan; b. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh Pembekal dan mengemukakan status kemajuan; dan c. Memaklumkan insiden keselamatan siber kepada pembekal oleh pemilik sistem seperti yang dikehendaki dalam perjanjian bagi penyelesaian insiden.	Pemilik Sistem, PICT dan Pembekal
PKSMOT-K11/06 Menguruskan Perubahan Kepada Perkhidmatan Pembekal		
	Perubahan kepada peruntukan perkhidmatan oleh Pembekal yang disebabkan oleh perubahan pada PKS MOT, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan data dan maklumat, sistem penyampaian dan proses perkhidmatan yang terlibat dan risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan dalam perjanjian dengan Pembekal; b. Perubahan yang dilakukan oleh MOT bagi meningkatkan perkhidmatan selaras dengan	Pemilik Sistem, PICT dan Pembekal

	penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c. Perubahan dalam perkhidmatan Pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran Pembekal dan subkontraktor.	

KAWALAN 12 : RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

PKSMOT - K12 **Objektif**		
Untuk memastikan semua insiden dikendalikan dengan konsisten, cepat, tepat dan berkesan termasuk saluran komunikasi keselamatan dan *security events* bagi memastikan sistem ICT MOT dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej MOT dan sistem penyampaian perkhidmatan.		
PKSMOT - K12/01 Mekanisme Pelaporan Insiden Keselamatan ICT		
	a. Pelaporan Semua insiden keselamatan ICT yang berlaku mesti dilaporkan segera kepada CSIRT MOT untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan bagi mengelakkan kerosakan bahan bukti tanpa melaksanakan tindakan secara sendirian berdasarkan kepada Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022. Semua maklumat adalah **SULIT**, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. Antara insiden keselamatan ICT yang perlu dilaporkan adalah: i. maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak- pihak yang tidak diberi kuasa; ii. sistem maklumat digunakan tanpa kebenaran atau yang disyaki sedemikian; iii. kata laluan atau mekanisme kawalan akses yang hilang, dicuri, didedahkan atau yang disyaki sedemikian; iv. berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali	ICTSO, Pengguna, CSIRT MOT

	gagal berfungsi atau dicapai, dan komunikasi tersalah hantar; dan v. berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka yang boleh menjejaskan keselamatan ICT. b. Pelaporan NACSA i. ICTSO melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT sekiranya perlu; dan ii. Pasukan CSIRT MOT dengan persetujuan ICTSO akan menghubungi NACSA untuk melaporkan atau mendapatkan bantuan apabila wujud potensi insiden atau berlaku sebarang insiden keselamatan ICT. c. Tindakan Dalam Keadaan Berisiko Tinggi Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak. d. ICTSO melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT sekiranya perlu. e. Insiden Keselamatan Sistem Pentadbir sistem yang terlibat mesti melaporkan sebarang kejadian yang melibatkan keselamatan ICT kepada CSIRT MOT.	

PKSMOT - K012/02 Prosedur Pengurusan dan Pengendalian Insiden Keselamatan ICT		
	Pasukan CSIRT MOT perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur pengurusan pelaporan dan pengendalian insiden keselamatan ICT MOT seperti di di **Lampiran 3 - Carta Alir Proses Kerja Pelaporan Insiden Keselamatan Siber** selaras dengan Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam). CSIRT MOT menerima aduan atau laporan daripada pengguna, laporan yang dikesan daripada pihak NACSA atau laporan daripada sumber lain. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada pihak NACSA. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguatkuasa undang- undang. CSIRT MOT yang diketuai oleh ICTSO akan menjalankan tindakan pengendalian secara capaian jauh (*remote*) atau *on-site.* Sekiranya laporan tersebut memerlukan bantuan pihak NACSA, permohonan akan dihantar bagi mendapatkan maklum balas pihak NACSA. Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan akan dihantar melalui pihak NACSA dan khidmat nasihat akan disalurkan. CSIRT MOT seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya DRP perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada Pengurus ICT bagi mengaktifkan DRP. Laporan insiden yang tidak memerlukan PKP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan.	ICTSO, CSIRTMOT

	Pengendalian insiden keselamatan ICT perlu diuruskan dengan cepat, teratur dan berkesan, mengikut prosedur dengan mengambil kira kawalan-kawalan berikut: a. mengenal pasti semua jenis insiden keselamatan ICT; b. mematuhi Pelan Pemulihan Bencana (DRP); c. menyimpan jejak audit dan memelihara bahan bukti dan rekod; d. menyediakan tindakan pencegahan supaya insiden serupa tidak berulang; dan e. memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

KAWALAN 13 : KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

PKSMOT - K13 **Objektif**		
Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
PKSMOT - K13/01 Pengurusan Kesinambungan Perkhidmatan		
	Pengurusan Kesinambungan Perkhidmatan (PKP) ialah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej MOT terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan MOT di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Ketua Jabatan adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT MOT. Pelan PKP terdiri daripada tiga (3) pelan utama iaitu Kumpulan Tindak Balas Kecemasan (ERT), Pelan Komunikasi Krisis (CCP) dan Pelan pemulihan Bencana (DRP). Pelan PKP perlu dibangunkan dan mengandungi perkara-perkara berikut: a. senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; b. senarai pengguna berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan pegawai yang tidak dapat hadir	Pasukan DRP MOT

	untuk menangani insiden; 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 perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Pelan PKP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes 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 pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. MOT hendaklah memastikan salinan pelan PKP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

PKSMOT - K13/01/01 Pelan Pemulihan Bencana		
	Pelan Pemulihan Bencana hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian: a. mengenal pasti semua tanggungjawab dan prosedur kecemasan dan pemulihan; b. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. mendokumentasikan proses dan prosedur yang telah dipersetujui; d. mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; e. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; f. membuat *backup*; dan g. menguji dan mengemaskini pelan sekurang- kurangnya setahun sekali.	Pasukan DRP MOT

PKSMOT - K13/02 *Redundancy*		
	Semua sistem aplikasi dan perkakasan yang kritikal hendaklah mempunyai kemudahan *redundancy* dan diuji (*failover test*) keberkesanannya mengikut keperluan.	Pengurus ICT, Pentadbir Sistem

KAWALAN 14 : PEMATUHAN

PKSMOT - K14 **Objektif**		
Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran kepada PKS MOT.		
PKSMOT - K14/01 Pematuhan Polisi		
	Setiap pengguna di MOT hendaklah membaca, memahami dan mematuhi PKS MOT dan undang-undang atau peraturan-peraturan lain yang berkaitan. Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga di MOT adalah seperti di **Lampiran 4**. Perkara yang perlu dipatuhi adalah seperti berikut: a. semua perlembagaan, undang-undang, peraturan, perjanjian yang dimeterai dan lain-lain perkara yang relevan kepada keselamatan sistem maklumat dan organisasi hendaklah dikenal pasti, didokumentasikan dan dikemas kini; b. peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan perjanjian mengenai penggunaan material yang tertakluk kepada hak milik harta intelek; c. rekod penting hendaklah dilindungi daripada hilang, rosak dan dipalsukan selaras dengan keperluan undang-undang, peraturan dan keperluan perjanjian MOT;	Pengguna

	d. perlindungan ke atas data dan maklumat privasi hendaklah mematuhi perundangan, peraturan dan terma perjanjian jika perlu; e. penyalahgunaan pemprosesan maklumat adalah tidak dibenarkan; dan f. penggunaan kriptografi dikawal selaras dengan perjanjian, perundangan dan peraturan yang berkuat kuasa.	
PKSMOT - K14/02 Pematuhan kepada Polisi, Peraturan dan Penilaian Teknikal Keselamatan		
	ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi polisi, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi piawaian pelaksanaan keselamatan. Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment* (SPA) mestilah dijalankan oleh individu yang kompeten dan dibenarkan.	ICTSO

PKSMOT - K14/03 Pematuhan Keperluan Audit		
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dikawal dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO
PKSMOT - K14/04 Pelanggaran Perundangan		
	Pelanggaran polisi ini boleh diambil tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-perintah Am Bab "D" - Peraturan-peraturan Pegawai Awam (Kelakuan Dan Tatatertib).	Pengguna

KAWALAN 15 : RISIKAN ANCAMAN *(THREAT INTELLIGENCE)*

PKSMOT - K15 **Objektif**		
Untuk memberi kesedaran tentang persekitaran ancaman organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.		
PKSMOT - K15/01 Risikan Ancaman *(Threat Intelligence)*		
	a. Risikan Ancaman ialah kerjasama dengan semua pasukan keselamatan maklumat dalam organisasi MOT; b. Perisian Risikan Ancaman boleh digunakan untuk pengumpulan risikan yang berkaitan bersama dengan kerjasama dengan semua pasukan keselamatan maklumat dalam organisasi; dan c. Sumber dalaman dan luaran boleh digunakan untuk pengumpulan maklumat risikan. Sumber tersebut mestilah relevan, tepat pada masanya dan boleh dipercayai.	Pengguna

KAWALAN 16 : KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN *CLOUD*

PKSMOT - K16		
Objektif		
Untuk menentukan dan mengurus keselamatan maklumat untuk penggunaan perkhidmatan *cloud.*		
PKSMOT - K16/01 Keselamatan Maklumat Bagi Penggunaan Perkhidmatan *Cloud*		
	Peranan dan tanggungjawab dalam persekitaran *cloud* ● Tanggungjawab dan peranan keselamatan maklumat yang dikongsi dalam penggunaan *cloud* di MOT harus diperuntukkan kepada pihak yang dikenal pasti, didokumenkan, dikomunikasikan dan dilaksanakan oleh kedua-dua pengguna dan pembekal perkhidmatan cloud. Mengalih keluar aset pelanggan perkhidmatan cloud ● Aset pengguna perkhidmatan *cloud* yang berada di premis pembekal perkhidmatan *cloud* harus dialih keluar dan dikembalikan jika perlu, selepas penamatan terma dan syarat perkhidmatan di MOT. Keselamatan operasi pentadbir ● Prosedur untuk operasi pentadbiran persekitaran pengkomputeran *cloud* harus ditakrifkan, didokumenkan dan dipantau. Pemantauan untuk Perkhidmatan *cloud* ● Pengguna perkhidmatan *cloud* harus mempunyai keupayaan untuk memantau aspek tertentu operasi perkhidmatan *cloud* yang digunakan oleh pengguna perkhidmatan *cloud*. Pengasingan dalam persekitaran maya (virtual environment) a. Persekitaran maya pengguna perkhidmatan *cloud* yang berjalan pada pembekal perkhidmatan *cloud* harus dilindungi daripada pelanggan perkhidmatan cloud yang lain dan pihak yang tidak dibenarkan.	Pengguna dan Pembekal

GLOSARI

Glosari	
Active Directory (AD)	Teknologi *Microsoft* yang digunakan untuk mengurus komputer dan perkakasan lain dalam rangkaian.
Antivirus	Perisian yang mengimbas virus pada media storan, seperti cakera keras (hard disk) dan *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari suatu tempat ke suatu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
Aset ICT	Peralatan ICT milik kerajaan dan sewaan termasuk komputer meja, komputer riba, pencetak dan pengimbas, media storan, *server*, *router*, *firewall*, rangkaian dan lain-lain.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh: di antara cakera keras dan PC utama) dalam jangka masa yang ditetapkan.
BYOD	*Bring Your Own Device*
CCTV	*Closed-circuit television* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CSIRT Agensi	*Cyber Security Incident Response Team* Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
CDO/CIO	*Chief Digital Officer/Chief Information Officer* Ketua Pegawai Digital/Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi

Glosari	
	menyokong hala tuju sesebuah organisasi bagi mewujudkan budaya kerja yang dipacu oleh digital.
Clear Desk dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat terperingkat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
Data-at-rest	*Data-at-rest* (data-dalam-simpanan) Data yang tidak aktif yang disimpan secara fizikal dalam bentuk digital (contohnya pangkalan data, gudang data, hamparan, arkib dan sebagainya).
Data-in-motion	*Data-in-motion* (data-dalam-pergerakan) Data-dalam-pergerakan atau data transit maklumat digital yang sedang dalam proses pergerakan di dalam atau antara sistem komputer.
Data-in-use	*Data-in-use* (data-dalam-penggunaan) Data yang digunakan adalah data yang sedang diperbaharui, diproses, dihapus, diakses atau dibaca oleh sistem. Jenis data ini tidak disimpan secara pasif, tetapi bergerak aktif melalui infrastruktur IT.
Data masking	*Data masking* ialah kaedah penyembunyian data asli yang digunakan untuk tujuan pengujian dan latihan.
Defence-in-depth	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
DRC	*Disaster Recovery Centre* Pusat Pemulihan Bencana
DRP	*Disaster Recovery Plan* Pelan Pemulihan Bencana

Glosari	
Encryption	Penyulitan atau enkripsi. Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat *(information theft/espionage),* penipuan *(hoaxes).*
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
ICT	*Information and Communication Technology*
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
ISDN	*Integrated Services Digital Networks* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer 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.

Glosari	
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
Intrusion Detection System (IDS)	Sistem Pengesanan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegahan Pencerobohan Perkakasan keselamatan yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Berperanan bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Sebagai contoh, Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
ISMS	*Information Security Management System*
MOT	Organisasi MOT merangkumi bahagian-bahagian seperti berikut: 1. Bahagian Akaun (BA); 2. Bahagian Darat (BD); 3. Bahagian Maritim (BM); 4. Bahagian Pembangunan (BP); 5. Bahagian Pengurusan Maklumat (BPM); 6. Bahagian Pengurusan Sumber Manusia (BPSM); 7. Bahagian Pentadbiran (BT); 8. Bahagian Perancangan Strategik dan Antarabangsa (BPSA); 9. Bahagian Perolehan dan Kewangan (BPK); 10. Bahagian Udara (BU); 11. Biro Siasatan Kemalangan Udara (BSKU); 12. Pejabat Penasihat Undang-undang (PPUU); 13. Unit Audit Dalam (UAD); dan 14. Pusat Logistik Negara (PLN).
Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman keselamatan ICT yang boleh menjejaskan kelancaran operasi dan sistem ICT MOT.

Glosari	
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (piawaian format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
KPKK	Ketua Pegawai Keselamatan Kerajaan
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Lightning arrestor	Alat yang digunakan untuk mencegah daripada ancaman kilat.
Lock	Mengunci komputer.
Log out	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Merupakan perisian hasad atau jahat yang memasuki sistem komputer dan menyebabkan risiko keselamatan seperti kerosakan komputer, gangguan capaian Internet dan sebagainya tanpa disedari oleh 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.
Mobile Code	*Mobile code* merupakan perisian yang boleh dipindahkan antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh *Java Applet, ActiveX* dan sebagainya pada pelayar Internet.
MySEAL	*National Trusted Cryptographic Algorithm List* Senarai Algoritma Kriptografi Terpercaya Negara (MySEAL) ialah projek untuk membangunkan portfolio algoritma kriptografi terpercaya negara.
NACSA	*National Cyber Security Agency* Agensi Keselamatan Siber Negara
Outsource	Maklumat yang diproses dan diperoleh di luar daripada sesuatu organisasi atau struktur kerja.

Glosari	
Peripheral	Aset yang digunakan untuk menyokong pemprosesan maklumat.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Pengguna	Pengguna terdiri daripada warga MOT dan pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT MOT.
Pegawai Aset ICT	Pegawai Aset ICT merupakan pegawai yang mahir dan berkelayakan mengenai bidang pengkomputeran dan dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab: - a. Perolehan Aset; b. Penerimaan Aset; c. Pendaftaran Aset; d. Penggunaan, Penyimpanan dan Pemeriksaan; e. Penyelenggaraan; f. Pelupusan; dan g. Penyelenggaraan Sistem Aplikasi Teras.
Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan daripada segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
Pegawai Keselamatan	*Memastikan keselamatan perlindungan di jabatan terjamin sepanjang masa.*
Pihak Luaran	Pihak luaran terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan atau pelawat yang mengunjungi MOT atas urusan rasmi.
PKI	*Public-Key Infrastructure* Infrastruktur Kunci Awam
PKP	Pengurusan Kesinambungan Perkhidmatan

Glosari	
Pusat Data MOT	Pengurusan pusat data MOT
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.
Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada negara.
Restoration	Pemulihan ke atas data.
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 ia tidak digunakan dalam jangka masa tertentu.
Server	Pelayan
Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
Switch	Alat yang boleh menapis (*filter*) dan memajukan (*forward*) isyarat paket data antara segmen rangkaian LAN.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.
Threat	*Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.*

Glosari	
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan 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.
WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
Worm	Sejenis virus yang boleh beraplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

LAMPIRAN 1

KEMENTERIAN PENGANGKUTAN MALAYSIA

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER KEMENTERIAN PENGANGKUTAN (MOT)

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian/Unit : .....

Organisasi (selain warga MOT) : .....

No. Kontrak (jika berkaitan) : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber MOT; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Disahkan oleh,

.....

Pegawai Keselamatan ICT (ICTSO)

b/p Ketua Setiausaha

Kementerian Pengangkutan (MOT)

Tarikh :.....

LAMPIRAN 2

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 mendapat 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 : _____

Cop Jabatan / Organisasi :

PERAKUAN UNTUK DITANDATANGANI OLEH KONTRAKTOR YANG TERLIBAT DENGAN PROJEK KERAJAAN MENURUT AKTA RAHSIA RASMI 1972

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

Saya faham bahawa segala maklumat 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 mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila tamat projek Kerajaan.

Tandatangan : _____

Nama (huruf besar) : _____

No. Kad Pengenalan : _____

Jawatan : _____

Jabatan / Organisasi : _____

Tarikh : _____

Disaksikan oleh : _____
(Tandatangan)

Nama (huruf besar) : _____

No. Kad Pengenalan : _____

Jawatan : _____

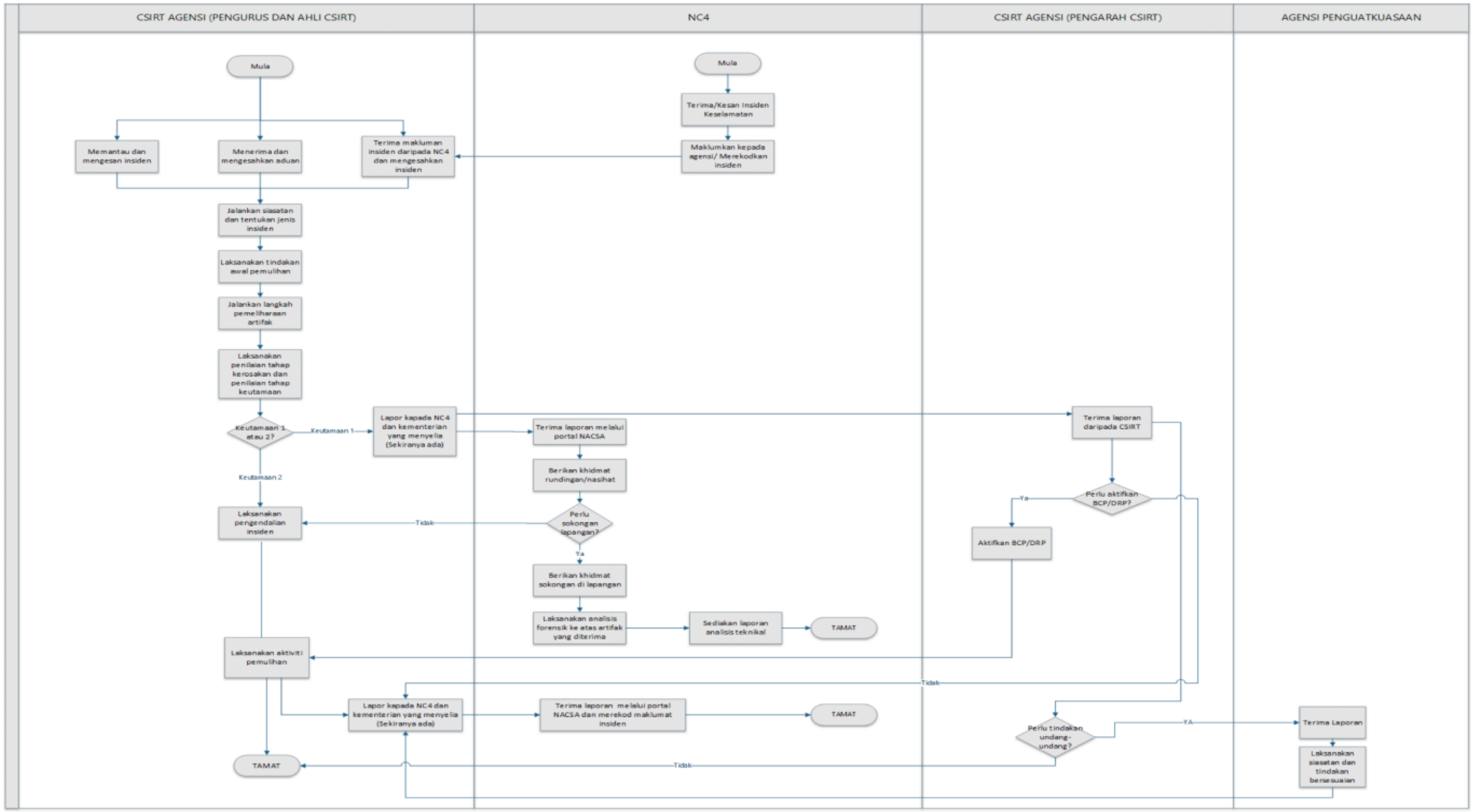
Jabatan / Organisasi : _____

Tarikh : _____

Cop Jabatan / Organisasi :

LAMPIRAN 3

CARTA ALIR PROSES KERJA PELAPORAN INSIDEN KESELAMATAN SIBER



LAMPIRAN 4

SENARAI PERUNDANGAN DAN PERATURAN

1.	Akta Tandatangan Digital 1997;
2.	Akta Rahsia Rasmi 1972;
3.	Akta Jenayah Komputer 1997;
4.	Akta Hak cipta (Pindaan) Tahun 1997;
5.	Akta Komunikasi dan Multimedia 1998;
6.	Akta 709 – Akta Perlindungan Data Peribadi 2010;
7.	Akta 658 – Akta Perdagangan Elektronik 2006;
8.	Akta 629 – Akta Arkib Negara 2003;
9.	Akta 606 – Akta Cakera Optik 2000;
10.	Akta 298 – Kawasan Larangan Tempat Larangan 1959;
11.	Akta 56 – Akta Keterangan 1950;
12.	Akta Keselamatan Siber 2024 [Akta 854];
13.	Arahan Keselamatan;
14.	Arahan Perbendaharaan;
15.	Arahan Teknologi Maklumat 2007
16.	Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara;
17.	Arahan 24 – Dasar dan Mekanisme Pengurusan Krisis Siber Negara;
18.	Dasar Pengurusan Rekod dan Arkib Elektronik
19.	Etika Penggunaan E-mel dan Internet MOT;
20.	Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU);
21.	Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013;
22.	Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006;
23.	Garis Panduan Pengurusan Rekod;
24.	Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi;
25.	Guideline to Determine Information Security Professionals Requirement for the CNII Agencies /Organisations;
26.	National Cyber Security Policy (NCSP);
27.	Panduan Pelaksanaan Audit ISMS Sektor Awam;
28.	Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";
29.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 bertajuk "Pengurusan Laman Web Agensi Sektor Awam";

30.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";
31.	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007";
32.	Pekeliling Transformasi Pentadbiran Awam Bilangan 3 Tahun 2017: Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan;
33.	Pekeliling Am Bilangan 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam;
34.	Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan;
35.	Perintah-Perintah Am;
36.	Pelan Pengurusan Pemulihan Bencana MOT;
37.	PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua);
38.	Polisi Keselamatan Siber MAMPU
39.	Pekeliling Perbendaharaan AM 2 Tahun 2018: Tatacara Pengurusan Aset Alih Kerajaan;
40.	Rancangan Malaysia Ke-12;
41.	Surat Arahan KPPA Tindakan Ke Atas Penjawat Awam Yang Mendedahkan/Membocorkan Dokumen/Maklumat Terperingkat Kerajaan bertarikh 28 Januari 2015;
42.	Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk "Penggunaan Media Jaringan Sosial di Sektor Awam";
43.	Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam yang bertarikh 26 Januari 2015;
44.	Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat yang bertarikh 24 November 2010;
45.	Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
46.	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
47.	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
48.	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;
49.	Surat Aku Janji;
50.	Surat Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2015 bertajuk "Panduan Pelaksanaan Program Turun Padang Sektor Awam";
51.	Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology* ICT Kerajaan SPP 3/2013;

52.	Surat Pekeliling Am Bilangan 8 Tahun 2024 - Garis Panduan Pengurusan dan Pengendalian Rahsia Rasmi Dalam Perkhidmatan Awam bertarikh 22 Julai 2024
53.	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi 1.0 April 2016;
54.	Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019
55.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 - Dasar Pengkomputeran Awan Sektor Awam bertarikh 10 Jun 2021
56.	Surat Pekeliling Am Bilangan 2 Tahun 2021- Garis Panduan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam bertarikh 9 Ogos 2021
57.	Pekeliling Perbendaharaan (PK 2.6) - Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam
58.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2021 - Dasar Perkongsian Data Sektor Awam
59.	Surat Pekeliling Am Bilangan 4 Tahun 2022 - Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam
60.	Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022
61.	Tatacara Penggunaan E-Mel Dan Internet MOT
62.	Garis Panduan Penggunaan Capaian VPN Dan Komunikasi Sidang Video MOT
63.	Surat Pekeliling Am Bilangan 7 Tahun 2024 - Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi dan Komunikasi (ICT) Sektor Awam bertarikh 16 Julai 2024
64.	Surat Pekeliling Am Bilangan 3 Tahun 2024-Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024
65.	Pekeliling Perbendaharaan (PK 7.6) - Perolehan Berkaitan ICT dan Rangkaian Internet