POLISI KESELAMATAN SIBER

ANGKATAN PERTAHANAN AWAM MALAYSIA (APM)

JABATAN PERDANA MENTERI (JPM)

1 OKTOBER 2022

SEJARAH DOKUMEN

Versi	Kelulusan	Tarikh Kuat Kuasa
1.0	JPICT APM	26 Oktober 2022

SENARAI KANDUNGAN

BAHAGIAN : 01

PENGENALAN

Polisi Keselamatan Siber Angkatan Pertahanan Awam Malaysia (APM) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi semasa menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Polisi ini juga menerangkan kepada pengguna mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT dan maklumat di ruang siber APM.

OBJEKTIF

PKS APM diwujudkan untuk mengurus dan memastikan kesemua komponen keselamatan diambilkira dalam usaha melindungi maklumat dalam ruang siber APM. Ia juga bertujuan untuk menjamin kesinambungan urusan Jabatan dengan meminimumkan kesan insiden keselamatan ICT di samping memudahkan perkongsian maklumat sesuai dengan keperluan operasi APM.

Objektif utama PKS adalah seperti berikut:

1. Melindungi aset ICT APM daripada penyalahgunaan oleh pengguna;
2. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan aset ICT;
3. Melindungi maklumat atau data yang disimpan dan diproses dalam bentuk digital atau ruang siber Jabatan;
4. Melindungi kepentingan pihak-pihak yang bergantung kepada infrastruktur dan sistem aplikasi ICT daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan;
5. Menjamin kesinambungan operasi Jabatan yang berlandaskan ICT dengan meminimumkan kesan insiden keselamatan seperti kerosakan, kehilangan atau kemusnahan aset ICT Jabatan; dan
6. Meningkatkan tahap keyakinan pihak berkepentingan terhadap APM.

PENYATAAN POLISI

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat 7 komponen asas keselamatan ICT, iaitu

1. Melindungi maklumat rahsia rasmi dan maklumat rasmi APM dari capaian tanpa kuasa yang sah;

2. Mengesan ancaman serangan siber melalui pemantauan dan kawalan berterusan terhadap penggunaan rangkaian;

3. Memastikan tindak balas terhadap ancaman siber diambil tindakan dan dilapor kepada pihak yang berkaitan;

4. Melaksanakan tindakan pemulihan terhadap kerosakan yang disebabkan oleh serangan siber dan kegagalan sistem untuk menjamin tahap ketersediaan, ketepatan dan integriti maklumat;

5. Menjamin setiap maklumat adalah tepat dan sempurna;

6. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

7. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

PKS APM merangkumi perlindungan ke atas semua bentuk maklumat eletronik 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 diakses 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; dan

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

Selain itu, analisa tahap risiko aset ICT dikenalpasti, seterusnya mengambil tindakan untuk merancang dan mengawal risiko berkenaan.

SKOP POLISI

Ruang siber ditakrifkan sebagai sistem-sistem ICT, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem ini secara fizikal atau maya, serta persekitaran fizikal sistem-sistem tersebut disimpan. Maklumat yang dipindahkan dari ruang siber ke ruang fizikal (melalui cetakan, salinan tulisan tangan serta rakaman foto menggunakan peralatan fotografik) adalah di luar skop polisi ini dan hendaklah ditangani dengan peraturan sedia ada.

Keselamatan siber ditakrifkan sebagai keadaan bagi segala urusan menyedia dan membekalkan perkhidmatan digital yang berasaskan kepada sistem ICT berjalan secara berterusan.

Aset ICT adalah terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. PKS APM menetapkan keperluan-keperluan asas keselamatan 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 APM.

PKS APM merangkumi perlindungan ke atas semua bentuk maklumat ICT Kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpankan, dijanakan, diakses, diedarkan dan yang dibuat salinan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. **Data dan Maklumat**

   Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif jabatan contoh: sistem dokumentasi, profil-profil pelanggan, prosedur operasi, rekod-rekod jabatan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

2. Perkakasan dan Peranti Fizikal

Semua aset yang digunakan untuk menyokong perkhidmatan digital dan pemprosesan maklumat di APM seperti komputer peribadi, komputer riba, pencetak, media storan, server, *firewall*, peralatan multimedia & komunikasi, dan alat-alat prasarana seperti *Uninterruptible Power Supply* (UPS) dan lain-lain;

3. Sistem Aplikasi dan Perisian

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

4. Perkhidmatan

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

(a) Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
(b) Sistem halangan akses seperti sistem kad akses;
(c) Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegahan kebakaran dan lain-lain. dan

5. Manusia

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

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

PRINSIP-PRINSIP

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

1. **Prinsip "Perlu Tahu"**

   Hak penggunaan aset ICT hanya diberikan kepada pengguna yang dibenarkan sahaja berdasarkan prinsip "Perlu Tahu" iaitu untuk tujuan pelaksanaan tugasnya sahaja. Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan adalah dihadkan kepada masa, lokasi dan status bekerja pengguna tersebut.

2. **Hak Capaian Minimum**

   Hak capaian kepada pengguna hanya diberi pada tahap yang paling minimum iaitu capaian untuk membaca dan atau melihat sahaja bagi tujuan pelaksanaan tugasnya. Kelulusan khas diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah dan menghapus sesuatu data atau maklumat.

3. **Akauntabiliti atau Kebertanggungjawaban**

   Warga APM khususnya dan 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 sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

   Akauntabiliti atau tanggungjawab pengguna termasuklah:

   (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

   (b) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

(c) Menentukan maklumat sedia untuk digunakan;

(d) Menjaga kerahsiaan kata laluan;

(e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

(f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

(g) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

4. Pengasingan Tugas

Tujuan pengasingan tugas seperti mewujud, memadam, mengemaskini, mengubah dan mengesahkan data diasingkan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, dimanipulasi dan seterusnya, mengekalkan integriti dan kebolehsediaan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program, kemudahan sistem dan komunikasi, manakala pemisahan perubahan pada konfigurasi dan keperluan sistem.

Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

(a) Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;

(b) Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji dan dibuat penerimaan pengguna; dan

(c) Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

5. Pengauditan

Tujuan pengauditan adalah untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router, firewall*, dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*. Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta- merta.

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

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

a. Mengesan pematuhan atau pelanggaran keselamatan;

b. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran keselamatan; dan

c. Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran keselamatan.

6. Pematuhan

Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang pelanggaran dasar. Pematuhan kepada Polisi Keselamatan ICT APM boleh dicapai melalui tindakan berikut:

(a) Mewujud proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan;

(b) Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah- langkah keselamatan ICT yang dikenalpasti;

(c) Melaksana program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan

(d) Menguatkuasa amalan melapor sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

7. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:

(a) Merumus dan menguji Pelan Pemulihan Bencana – *(Disaster Recovery Plan)*; dan

(b) Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan baik dalam penggunaan ICT seperti menghapuskan virus, langkah- langkah pencegahan kebakaran dan amalan *clear desk*.

8. Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisme keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat di mana di tahap minimum, mengandungi langkah-langkah berikut;

(a) Sambungan kepada internet - Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisme pusat untuk mengurus, menguatkuasa dan mengawas sebarang bahaya keselamatan. Melalui sistem ini, semua trafik dalaman hendaklah melalui *gateway firewall* yang diurus secara berpusat. Semua trafik dari luar ke dalam hendaklah juga melalui laluan ini atau melalui kumpulan modem yang dikawal secara berpusat. Dengan itu, penggunaan modem dalaman tidak dibenarkan;

(b) *Backbone* Rangkaian – *Backbone* rangkaian akan hanya mengendalikan trafik yang telah dikod untuk meminimumkan intipan;

(c) Rangkaian APM – Semua rangkaian APM akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengkod semua trafik di antara rangkaian APM dengan rangkaian di peringkat yang seterusnya atau pusat data; dan

(d) Pelayan APM – Semua data dan maklumat yang kritikal atau sensitif akan hanya disimpan di pelayan APM atau di pelayan yang diurus secara pusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitif akan dikodkan.

BAHAGIAN : 02

PEMBANGUNAN DAN PENYELENGGARAAN POLISI

0101 – Polisi Keselamatan Siber		
Objektif Memastikan hala tuju dan sokongan pengurusan terhadap keselamatan siber selaras dengan keperluan APM dan perundangan yang berkaitan.		
PKS-010101	**Pelaksanaan Polisi**	**Tindakan**
	Pelaksanaan polisi ini akan dilaksanakan oleh Timbalan Ketua Pesuruhjaya (Pengurusan) APM selaku Ketua Pegawai Maklumat (CIO) dengan dibantu oleh Pengurus ICT, Pegawai Keselamatan ICT(ICTSO) dan semua Ketua Bahagian/Unit/ Cawangan di APM.	TKPP
PKS-010102	**Penyebaran Polisi**	**Tindakan**
	Polisi ini perlu disebarkan kepada semua pengguna di APM (termasuk warga kerja, pembekal, pakar runding dan lain-lain).	ICTSO
PKS-010103	**Penyelenggaraan Polisi**	**Tindakan**
	PKS APM adalah tertakluk kepada kajian semula secara berkala selaras dengan perubahan teknologi, aplikasi serta peraturan dan perundangan yang sedang berkuat kuasa.	ICTSO

	Prosedur bagi penyelenggaraan polisi adalah seperti berikut: a. Mengenalpasti dan menentukan pindaan yang diperlukan sekurang-kurangnya 1 kali setahun atau mengikut keperluan semasa; b. Mengemukakan cadangan pindaan kepada Pengurus ICT; c. Mengemukakan polisi yang telah dikaji dan dipinda untuk persetujuan CIO APM; dan d. Polisi yang telah dipersetujui hendaklah dimaklumkan kepada semua pengguna.	
PKS-010104	**Pengecualian Polisi**	**Tindakan**
	PKS APM hendaklah dipatuhi oleh semua pengguna ICT di APM dan tiada pengecualian diberikan.	Semua pengguna APM

ORGANISASI KESELAMATAN SIBER

0201 – Infrastruktur Tadbir Urus		
Objektif Menerangkan struktur, peranan dan tanggungjawab tadbir urus yang terlibat dalam merancang, mengurus dan mengawal polisi serta fungsi yang berkaitan dengan keselamatan maklumat di APM.		
PKS-020101	**Ketua Jabatan**	**Tindakan**
	Peranan dan tanggjungjawab Ketua Pesuruhjaya APM adalah seperti berikut: a. Memastikan semua keperluan Jabatan bagi menjamin keselamatan siber adalah mencukupi; dan b. Memastikan pengurusan keselamatan siber dilaksanakan sepertimana yang ditetapkan dalam PKS APM.	KPj
PKS-020102	**Ketua Pegawai Maklumat (CIO) / Ketua Pegawai Digital (CDO)**	**Tindakan**
	Timbalan Ketua Pesuruhjaya (Pengurusan) APM adalah merupakan Ketua Pegawai Maklumat atau *Chief Information Officer* (CIO) dan Ketua Pegawai Digital atau *Chief Digital Officer* (CDO). Peranan dan tanggungjawab CIO adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber APM; b. Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber;	CIO/CDO

	c. Menentukan keperluan keselamatan siber; d. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan siber; e. Memastikan semua bahagian/unit/cawangan di APM mematuhi arahan mengenai pengurusan keselamatan siber serta meningkatkan pematuhan ke atas kehendak akta, arahan, peraturan dan prosedur berkaitan; dan f. Mengesah dan menentukan sama ada insiden siber yang berlaku perlu dilaporkan kepada agensi penguatkuasa undang-undang atau keselamatan berkaitan.	
PKS-020103	**Pegawai Keselamatan ICT (ICTSO)**	**Tindakan**
	Ketua Cawangan Teknologi Maklumat APM adalah merupakan Pegawai Keselamatan ICT. Peranan dan tanggungjawab ICTSO adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber APM; b. Mengurus keseluruhan program-program keselamatan siber organisasi; c. Menguatkuasakan Polisi Keselamatan Siber APM; d. Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber APM kepada semua pengguna; e. Mewujudkan garis panduan dan prosedur selaras dengan keperluan Keselamatan Siber APM; f. Melaksanakan pengurusan risiko;	ICTSO

	g. Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; h. Memberi amaran kepada semua pejabat negeri, daerah dan pusat Latihan terhadap kemungkinan berlakunya ancaman keselamatan siber serta memberi khidmat nasihat dan bantuan teknikal bagi menyediakan langkah-langkah perlindungan yang bersesuaian; i. Melaporkan insiden keselamatan siber kepada CERT APM atau/ dan GCERT, MAMPU dan memaklumkannya kepada CIO/CDO; j. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; k. Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar Polisi Keselamatan Siber APM; dan l. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan siber.	
PKS-020104	**Pengurus ICT**	**Tindakan**
	Ketua Cawangan Teknologi Maklumat APM adalah merupakan Pengurus ICT. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:	Pengurus ICT

	a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber APM; b. Memastikan kajian semula dan pelaksanaan kawalan keselamatan siber selaras dengan keperluan organisasi; c. Melaporkan sebarang perkara atau penemuan mengenai keselamatan siber kepada CIO untuk tindakan; d. Memastikan penyampaian rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber organisasi dilaksanakan; dan e. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai Pentadbir Sistem ICT yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas.	
PKS-020105	**Pentadbir Sistem ICT**	**Tindakan**
	Peranan dan tanggungjawab adalah termasuk seperti berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber APM; b. Menjaga kerahsiaan kata laluan; c. Menjaga kerahsiaan konfigurasi aset ICT; d. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai semua pengguna ICT APM yang gantung kerja, berhenti, bersara, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; e. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai	Pentadbir Sistem ICT

	pengguna luar dan pihak ketiga yang berhenti atau tamat projek; f. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan; g. Memantau aktiviti capaian harian pengguna; h. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran, membatalkan atau memberhentikannya dengan serta-merta, dan memaklumkan kepada Pengurus ICT untuk tindakan selanjutnya; i. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; dan j. Menyimpan dan menganalisis rekod jejak audit.	
PKS-020106	**Pengguna Dalaman**	**Tindakan**
	Peranan dan tanggungjawab adalah termasuk seperti berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber APM; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melaksanakan langkah-langkah perlindungan seperti berikut: - Menjaga kerahsiaan maklumat APM yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;	Pengguna Dalaman

	- Menjaga kerahsiaan kata laluan; - Memastikan maklumat berkaitan adalah tepat dan lengkap dari semasa ke semasa; dan - Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum. d. Menghadiri program-program kesedaran mengenai keselamatan ICT e. Mengawal aktiviti penggunaan media sosial seperti berikut: - Tidak memberi atau mendedahkan sebarang komen atau penyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar Kerajaan; - Tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan - Tidak menggunakan saluran media sosial hingga mengganggu fokus dalam mesyuarat dan urusan kerja.	

PENGURUSAN ASET

0301 – Akauntabiliti Aset		
Objektif Untuk memberikan perlindungan keselamatan yang bersesuaian kepada semua aset ICT		
PKS-030101	**Inventori Aset ICT**	**Tindakan**
	Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset dikenal pasti, dikelas, didokumen, diselenggara dan dilupuskan apabila tiba masanya di mana maklumat aset direkod dan dikemaskini dalam borang daftar harta modal dan inventori serta sentiasa dikemaskini; b. Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. Peraturan bagi pengendalian aset hendaklah dikenalpasti, didokumen dan dilaksanakan; dan d. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai Aset dan Pengguna

0302 – Pengurusan Data dan Maklumat		
Objektif Memastikan setiap data dan maklumat digital termasuk aliran berkaitan diberikan tahap perlindungan yang bersesuaian.		
PKS-030201	**Pengelasan Maklumat**	**Tindakan**
	Semua maklumat yang dijana atau dikumpul hendaklah dikelaskan mengikut kategori Maklumat Rasmi dan Maklumat Rahsia Rasmi oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Maklumat hendaklah dikelaskan kepada kategori berikut: a. Maklumat Rahsia Rasmi: Maklumat Rahsia Rasmi mempunyai erti yang diberikan kepadanya di bawah Akta Rahsia Rasmi 1972 [Akta 88]. Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972. b. Maklumat Rasmi; Maklumat Rasmi adalah maklumat yang diwujudkan, digunakan, diterima atau	Pegawai Pengelas dan Pengguna

	dikeluarkan secara rasmi oleh mana-mana agensi Kerajaan semasa menjalankan urusan rasmi. Maklumat Rasmi ini juga adalah merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara. c. Data Terbuka: Data Terbuka adalah maklumat yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan, tertakluk kepada pekeliling yang sedang berkuatkuasa.	
PKS-030202	**Pengendalian Maklumat**	**Tindakan**
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran,	Semua

	penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.	
PKS-030203	**Aliran Data**	**Tindakan**
	Aliran data dan komunikasi dalam APM hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.	Semua

KESELAMATAN SUMBER MANUSIA

0401 – Keselamatan Sumber Manusia Dalam Tugas Harian		
Objektif Untuk memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan APM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab dan peranan mereka dalam keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT.		
PKS-040101	**Sebelum Perkhidmatan**	**Tindakan**
	Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan APM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan ke atas keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan APM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan; dan c. Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

PKS-040102	Dalam Perkhidmatan	Tindakan
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan APM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan jabatan; b. Memastikan Latihan Kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pegawai dan kakitangan APM, sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; dan c. Memastikan adanya proses tindakan disiplin dan/ atau undang-undang ke atas pegawai dan kakitangan APM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan jabatan.	Semua
PKS-040103	**Bertukar Atau Tamat Perkhidmatan**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua aset ICT dikembalikan kepada jabatan 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	Semua

	ditetapkan jabatan dan/atau terma perkhidmatan.	

KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 – Keselamatan Fizikal dan Persekitaran		
Objektif Untuk menghalang capaian yang tidak dibenarkan, kerosakan dan gangguan terhadap persekitaran premis, peralatan dan maklumat.		
PKS-050101	**Kawalan Kawasan Terperingkat/ Terhad**	**Tindakan**
	Perkara yang perlu dipatuhi termasuk yang berikut: a. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; b. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; c. Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; d. Merekabentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana disebabkan oleh kuasa Tuhan atau perbuatan manusia; e. Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; f. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat	CIO, Pengurus ICT, ICTSO dan Cawangan Pengurusan Am, BKP

	lain dikawal dari mana-mana pihak yang diberi kebenaran memasukinya; g. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; h. Menghadkan jalan keluar masuk; dan i. Menyediakan tempat atau bilik khas untuk pelawat-pelawat;	
PKS-050102	**Kawalan Masuk Fizikal**	**Tindakan**
	Perkara yang perlu dipatuhi termasuk yang berikut: a. Setiap pengguna di Angkatan Pertahanan Awam hendaklah memakai atau mengekana pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan balik kepada Angkatan Pertahanan Awam apabila pengguna berhenti atau bersara; c. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan APM. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan d. Kehilangan pas mestilah dilaporkan dengan segera.	Semua

0502 – Keselamatan Dokumen		
Objektif Untuk melindungi maklumat Angkatan Pertahanan Awam dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.		
PKS-050201	**Dokumen**	**Tindakan**
	Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat serta pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit atau Terhad kepada dokumen; c. Satu sistem pengurusan dokumen terperingkat hendaklah diwujudkan bagi menerima, memproses, menyimpan da nmenghantar dokumen-dokumen tersebut supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak terperingkat; dan d. Menggunakan penyulitan (enkripsi) ke atas dokumen terperingkat yang disediakan dan dihantar secara elektronik.	Semua
PKS-050202	**Media Storan**	**Tindakan**
	Keselamatan media storan perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat	Semua

	rasmi dan rahsia rasmi APM. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat: a. Menyediakan ruang penyimpanan dan bekas-bekas keselamatan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Menghadkan akses kepada pengguna yang dibenarkan sahaja; c. Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan; dan d. Mengadakan sistem pengurusan media termasuk inventori, pergerakan, pelabelan dan *backup/restore.*	
PKS-050203	**Bahan-bahan Habis Guna**	**Tindakan**
	Keselamatan bahan-bahan habis guna terkawal perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat rasmi dan rahsia rasmi APM. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat: a. Menyediakan ruang penyimpanan dan bekas-	

	bekas keselamatan yang mempunyai ciri-ciri keselamatanbersesuaian dengan kandungan maklumat; b. Menghadkan akses kepada pengguna yang dibenarkan sahaja; dan c. Sebarang pelupusan hendaklah merujukan kepada tatacara pelupusan.	

0503 – Keselamatan Persekitaran

Objektif

Untuk melindungi aset ICT dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

PKS-050301 Kawalan Persekitaran		**Tindakan**
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh dan ubahsuai hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Perkara yang perlu dipatuhi adalah seperti berikut: a. Merancang dan menyediakan pelan keseluruhan pusat data termasuk ruang peralatan komputer, ruang percetakan dan ruang atur pejabat; b. Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Memasang peralatan perlindungan di tempat	Semua

	yang bersesuaian, mudah dikenali dan dikendalikan; d. Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpan aset ICT; e. Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT; dan g. Menyemak dan menguji semua peralatan perlindungan sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu	
PKS-050302	**Bekalan Kuasa**	**Tindakan**
	a. Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada peralatan ICT; b. Menggunakan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.	Semua
PKS-050303	**Prosedur Kecemasan**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan setiap pengguna membaca,	Semua dan Pegawai

	memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh Pegawai Keselamatan Jabatan; b. Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan Jabatan yang dilantik mengikut aras; c. Mengadakan, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa; dan d. Mengadakan latihan *fire drill* mengikut jadual	Keselamatan Jabatan
PKS-050304	**Keselamatan Kabel**	**Tindakan**
	Kabel elektrik dan telekomunikasi yang menyalurkan data atau menyokong sistem penyampaian perkhidmatan hendaklah dilindungi daripada pencerobohan dan kerosakan. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d. Membuat pelabelan kabel menggunakan kod tertentu bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	

0504 – Keselamatan Peralatan		
Objektif Untuk melindungi Peralatan ICT dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut		
PKS-050401 Peralatan ICT		**Tindakan**
	Perkara yang perlu dipatuhi termasuk yang berikut: a. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran peralatan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; d. Menempatkan dan mengawal perkakasan-perkakasan ICT supaya risiko ancaman dan bencana dari persekitaran serta percubaan menceroboh oleh pihak yang tidak diberi kebenaran dapat dikurangkan; e. Semua cadangan perolehan, penempatan dan pengubahsuaian perkakasan-perkakasan ICT hendaklah dirujuk kepada Jawatankuasa Pemanduan ICT APM terlebih dahulu; f. Semua cadangan pemindahan perkakasan - perkakasan ICT hendaklah dirujuk kepada Pengurus ICT; g. Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, kerosakan, pengubahsuaian tanpa kebenaran	Semua

	dan penyalahgunaan; h. 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; i. 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; j. Semua peralatan 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 APM, perlulah mendapat kelulusan Pegawai Aset ICT atau Pentadbir Aset ICT Bahagian bagi tujuan pemantauan; dan m. Aset ICT yang hilang hendaklah dilaporkan mengikut pekeliling perbendaharaan sedia ada.	
PKS-050402	**Penyelenggaraan Peralatan**	**Tindakan**
	Perkakasan hendaklah diselenggarakan betul bagi memastikan kebolehsediaan, kerahsiaan	Pengurus ICT dan CTM

	dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; b. Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan kepada pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
PKS-050403	**Peminjaman Perkakasan Untuk Kegunaan di Luar Pejabat**	**Tindakan**
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah perlu diambil termasuklah seperti berikut: a. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh jabatan bagi	Pegawai Aset ICT dan Pentadbir Aset Bahagian

	membawa keluar peralatan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan; b. Melindungi dan mengawal peralatan sepanjang masa; c. Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan d. Menyemak peralatan yang dipulangkan berada dalam keadaan baik.	
PKS-050404	**Pengendalian Peralatan Luar Yang Dibawa Masuk/Keluar**	**Tindakan**
	Bagi peralatan yang dibawa masuk ke premis APM, langkah keselamatan yang perlu diambil adalah seperti berikut: a. Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT APM; b. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh jabatan bagi membawa masuk/keluar peralatan; dan c. Menyemak peralatan yang dibawa keluar tidak mengandungi maklumat APM.	Pegawai Aset ICT dan Pentadbir Aset Bahagian
PKS-050405	**Pelupusan Perkakasan**	**Tindakan**
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Angkatan Pertahanan Awam dan ditempatkan di Ibu Pejabat Pertahanan Awam/Pejabat Negeri/ Daerah. Peralatan ICT yang hendak dilupuskan perlu	Semua dan Pengurusan ICT

	melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan APM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c. Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; f. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuatkuasa; dan g. Pengguna ICT adalah dilarang sama sekali daripada melakukan perkara-perkara seperti berikut:	

	- Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; - Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk, motherboard* dan sebagainya; - Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian atau unit di Angkatan Pertahanan Awam/ Pejabat Negeri/ Daerah; - Memindah keluar dari tempat asal mana-mana peralatan ICT yang hendak dilupuskan; - Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Angkatan Pertahanan Awam; dan - Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan seperti disket atau *thumdrive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
PKS-050406	***Clear Desk* dan *Clear Screen***	**Tindakan**
	Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan	Pengguna

	selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	

PENGURUSAN OPERASI DAN KOMUNIKASI

0601 – Pengurusan Prosedur Operasi		
Objektif Untuk memastikan kemudahan pemprosesan maklumat dan komunikasi adalah berfungsi dengan baik dan selamat dari sebarang ancaman atau gangguan.		
PKS-060101	**Tanggungjawab dan Prosedur Operasi**	**Tindakan**
	Perkara yang mesti dipatuhi termasuk yang berikut: a. Semua prosedur operasi hendaklah didokumenkan dengan jelas lagi teratur, dikemaskini dan sedia diguna pakai oleh pengguna mengikut keperluan; b. Setiap perubahan kepada sistem dan kemudahan pemprosesan maklumat mestilah dikawal; c. Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset jabatan; dan d. Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah kepada sistem yang sedang beroperasi.	Semua
PKS-060102	**Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-pihak Lain yang Berkepentingan**	**Tindakan**

	Perkara yang mesti dipatuhi termasuk yang berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang berkepentingan; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang berkepentingan perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c. Pengurusan kepada perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
PKS-060103	**Perancangan dan Penerimaan Sistem**	**Tindakan**
	Perkara yang mesti dipatuhi termasuk yang berikut: a. Penggunaan peralatan dan sistem mestilah dipantau, ditala (*tuned*) dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti akan dating untuk memastikan prestasi system di tahap optimum; dan b. Kriteria penerimaan untuk peralatan dan sistem baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya	Semua

	perlu dibuat semasa pembangunan dan sebelum penerimaan sistem.	
PKS-060104	**Perlindungan Dari *Malicius* dan *Mobile Code***	**Tindakan**
	Bertujuan untuk melindungi integrity maklumat dan perisian dari ancaman *malicious code* seperti *viruses, worms, trojan horses, logicbombs* dan lain-lain lagi. Perkara yang mesti dipatuhi termasuk yang berikut: a. Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi daripada *malicious code*; dan b. Dalam keadaan di mana *mobile code* dibenarkan, konfigurasinya hendaklah memastikan bahawa ia beroperasi berdasarkan kepada dasar keselamatan yang jelas dan penggunaan *mobile code* yang tidak dibenarkan adalah dilarang sama sekali.	Semua
PKS-060105	***Backup***	**Tindakan**
	Bertujuan untuk mengekalkan integriti, kesediaan maklumat dan kemudahan pemprosesan maklumat. Perkara yang mesti dipatuhi termasuk membuat dan menguji secara berkala Salinan maklumat dan perisian berdasarkan kepada prosedur *backup*.	Semua

PKS-060106	Pengurusan Keselamatan Rangkaian	Tindakan
	Bertujuan untuk memastikan perlindungan keselamatan maklumat dalam rangkaian serta infrastruktur sokongan. Perkara yang mesti dipatuhi termasuk yang berikut: a. Rangkaian perlu dikawal, dipantau dan diurus sebaiknya, bertujuan untuk mengawal daripada sebarang ancaman bagi menjamin keselamatan sistem dan aplikasi yang mengguna rangkaian, termasuk maklumat yang dipindahkan melaluinya; dan b. ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenalpasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar.	Semua
PKS-060107	**Pemantauan Rangkaian Berpusat**	**Tindakan**
	Bertujuan untuk memastikan pemantauan rangkaian berpusat Kerajaan dapat berfungsi secara berkesan dan berterusan. APM hendaklah memastikan pemantauan dilaksanakan oleh Pemantauan Rangkaian Infrastruktur ICT Sektor Awam Malaysia (PRISMA) ke atas rangkaian APM agar dapat berfungsi secara berkesan dan berterusan.	Semua

PKS-060108	Pengendalian Media	Tindakan
	Bertujuan untuk memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan media secara tidak sah, yang boleh mengganggu aktiviti perkhidmatan. Perkara yang mesti dipatuhi termasuk yang berikut: a. Prosedur perlu disediakan untuk pengurusan media mudahalih; b. Media yang tidak digunakan perlu dilupuskan secara selamatmengikut prosedur yang telah ditetapkan; c. Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna; dan d. Dokumentasi sistem perlu dilindungi dari capaian yang tidak dibenarkan.	Semua
PKS-060109	**Pertukaran Maklumat**	**Tindakan**
	Bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian dalam jabatan dan mana-mana entiti luar terjamin. Perkara yang mesti dipatuhi termasuk yang berikut: a. Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;	Semua

	b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara jabatan dengan pihak luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dan jabatan; d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan e. Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat jabatan.	
PKS-060110	**Perkhidmatan E-Dagang (transaksi kewangan secara elektronik)**	**Tindakan**
	Bertujuan untuk memastikan keselamatan perkhidmatan e-dagang dan penggunaannya. Perkara yang mesti dipatuhi termasuk yang berikut: 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 salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan	Semua

	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.	
PKS-060111	**Perkhidmatan Kiosk**	**Tindakan**
	Bertujuan untuk memastikan keselamatan perkhidmatan kiosk dan penggunaannya. Perkara yang mesti dipatuhi termasuk yang berikut: a. Maklumat yang terlibat dalam kiosk 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.	Semua
PKS-060112	**Pemantauan**	**Tindakan**
	Bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	Pengurus ICT

	Perkara yang mesti dipatuhi termasuk yang berikut: a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator sistem perlu direkodkan; e. Kesalahan, kesilapan dan/atau penyalahgunaan perlu dilog, dianalisis dan diambil tindakan sewajarnya; dan masa yang berkaitan dengan sistem pemprosesan maklumat dalam organisasi atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	

KAWALAN CAPAIAN

0701 – Keperluan Kawalan Capaian		
Objektif Untuk mengawal capaian ke atas maklumat		
PKS-070101	**Keperluan Kawalan Capaian**	**Tindakan**
	Bertujuan mengawal capaian ke atas maklumat, kemudahan proses maklumat, dan proses perkhidmatan berdasarkan keperluan perkhidmatan dan keperluan keselamatan. Peraturan kawalan capaian hendaklah mengambil kira penyebaran dan pengesahan maklumat. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dankeselamatan. Perkara yang perlu dipastikan termasuk seperti berikut: a. Kawalan capaian ke atas maklumat dan proses perkhidmatan mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman danluaran; c. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat.	Pengurus ICT dan ICTSO

PKS-070102	Pengurusan Capaian Pengguna	Tindakan
	Bertujuan memastikan bahawa sistem maklumat dicapai oleh pengguna yang sah dan menghalang capaian yang tidak sah. Perkara yang perlu dipatuhi adalah termasuk : a. Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan; b. Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat; c. Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran ketua jabatan secara bertulis dan direkodkan; d. Pemilikan akaun dan capaian pengguna adalah tertakluk kepadaperaturan jabatan dan tindakan pengemaskinian dan/atau pembatalan hendaklah diambil atas sebab seperti berikut: - Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh ketua jabatan; - Pengguna bercuti atau bertugas di luar pejabat dalam satu tempoh yang lama seperti mana yang ditentukan oleh Ketua Jabatan; - Pengguna bertukar jawatan, tanggungjawab dan/atau bidang tugas; - Pengguna yang sedang dalam prosiding dan/atau dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib; dan	Semua

	- Pengguna bertukar, berpindah jabatan, bersara dan/atau tamat perkhidmatan. Aktiviti capaian oleh pengguna direkod, diselenggara dengan sistematik dan dikaji dari masa ke semasa. Maklumat yang direkod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.	
PKS-070103	**Tanggungjawab Pengguna**	**Tindakan**
	Bertujuan memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat. Perkara yang perlu dipatuhi adalah termasuk yang berikut: a. Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan; b. Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan c. Mematuhi amalan *clear desk policy* atau *clear screen policy*.	Semua
PKS-070104	**Kawalan Capaian Rangkaian**	**Tindakan**
	Bertujuan menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:	semua

	a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian organisasi, rangkaian organisasi lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan, yang menepati kesesuaianpenggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
PKS-070105	**Kawalan Capaian Sistem Pengoperasian**	**Tindakan**
	Bertujuan memastikan bahawa capaian ke atas sistem pengoperasian dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong perkara berikut: a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan organisasi; b. Mewujudkan audit trail ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *superuser*; c. Menjana amaran (alert) sekiranya berlaku pelanggaran ke atasperaturan keselamatan sistem; d. Menyedia kaedah sesuai untuk pengesahan capaian (authentication); dan e. Menghadkan tempoh penggunaan mengikut kesesuaian. Perkara yang perlu dipatuhi termasuk yang berikut:	Semua

	- Mengawal capaian ke atas sistem operasi menggunakan prosedur log-on yang terjamin; - 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; - Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; - Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan mengatasi sebarang kawalan sistem dan aplikasi; - Menamatkan sesebuah sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan; dan - Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
PKS-070106	**Kawalan Capaian Rangkaian**	**Tindakan**
	Bertujuan menghalang capaian tidak sah ke atas maklumat yang terdapat di dalam sistem aplikasi. Kawalan capaian hendaklah: a. Membenarkan pengguna mencapai aplikasi dan maklumat mengikut tahap capaian yang ditentukan; b. Menyediakan mekanisme perlindungan bagi	Semua

	menghalang capaian tidak sah ke atas aplikasi dan maklumat daripada utiliti yang sedia ada dalam sistem operasi dan perisian malicious yang berupaya melangkaui kawalan sistem; dan c. Tidak berkompromi dengan sebarang sistem yang berkongsi sumber. Perkara yang perlu dipatuhi termasuk yang berikut: a. Menghadkan capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna selaras dengan peraturan organisasi; dan b. Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem yang berklasifikasi tinggi.	
PKS-070107 Peralatan Mudah Alih dan Kerja Jarak Jauh		**Tindakan**
	Bertujuan memastikan keselamatan maklumat semasamenggunakan peralatan mudah alih dan kemudahan kerja jarak jauh. Perkara yang perlu dipatuhi termasuk yang berikut: a. Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; dan b. Mewujudkan peraturan dan garis panduan untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat.	Semua

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

0801 – Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat		
Objektif Untuk memastikan aspek keselamatan dikenalpasti dan diambilkira dalam semua system maklumat dan/atau perkhidmatan termasuk sistem pengoperasian, infrastruktur, sistem aplikasi dan sistem perisian. Aspek keselamatan ini mesti dikenalpasti, dijustifikasikan, dipersetujui dan didokumentasikan sebelum sesuatu sistem maklumat direkabentuk dan dilaksanakan.		
PKS-0080101	**Keperluan Keselamatan Sistem Maklumat**	**Tindakan**
	Bertujuan menjelaskan keperluan memastikan bahawa aspek keselamatan dikenal pasti, dipersetujui dan didokumen pada setiap peringkat perolehan, pembangunan dan penyelenggaraan. Perkara yang perlu dipatuhi adalah termasuk yang berikut: a. Pernyataan keperluan bagi sistem maklumat baru atau penambahbaikan ke atas sistem sedia ada hendaklah menjelaskan mengenai kawalan jaminan keselamatan.	Pemilik Sistem dan ICTSO
PKS-0080102	**Pemprosesan Aplikasi Dengan Tepat**	**Tindakan**
	Bertujuan memastikan kawalan keselamatan yang sesuai digarap dan dijalin ke dalam aplikasi bagi menghalang kesilapan, kehilangan, pindaan	Pemilik Sistem dan ICTSO

	yang tidak sah dan penyalahgunaan maklumat dalam aplikasi. Perkara yang perlu dipatuhi adalah termasuk yang berikut: a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin kesahihan dan ketepatan; b. Menggabungkan semakan pengesahan ke dalam aplikasi untuk mengenal pasti sebarang kerosakan maklumat sama ada disebabkan oleh ralat pemprosesan atau tindakan yang disengajakan; c. Mengenal pasti dan melaksanakan kawalan untuk mengesah dan melindungi integriti mesej dalam sistem aplikasi; dan d. Melaksanakan proses pengesahan ke atas *output* data bagi menjamin kesahihan dan ketepatan pemprosesan sistem aplikasi.	
PKS-0080103	**Kawalan Kriptografi**	**Tindakan**
	Bertujuan untuk melindungi kerahsiaan, kesahihan dan integriti maklumat melalui teknik kriptografi. Perkara yang perlu dipatuhi adalah termasuk membangun kawawaln kegunaan dan melaksanakan suatu peraturan kawalan kriptografi dan pengurusan kunci yang digunakan untuk menyokong teknik kriptografi bagi melindungi maklumat.	CTM dan Pengurus ICT

PKS-0080104	Keselamatan Fail-fail Sistem	Tindakan
	Bertujuan memastikan capaian ke atas fail- fail sistem dan kod sumber program adalah terkawal dan aktiviti-aktiviti sokongan dilaksanakan dalam kaedah yang selamat. Kawalan perlu diambil untuk mengelakkan pendedahan maklumat sensitif semasa proses pengujian dilaksanakan. Perkara yang perlu dipatuhi adalah termasuk yang berikut: a. Mewujudkan peraturan untuk mengawal pemasangan perisian ke dalam sistem yang sedang beroperasi; b. Melindungi dan mengawal data-data ujian; dan c. Menghadkan capaian ke atas kod sumber program.	CTM dan Pengurus ICT
PKS-0080105	**Keselamatan Dalam Proses Pembangunan dan Sokongan**	**Tindakan**
	Bertujuan memastikan keselamatan perisian sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan. Perkara yang perlu dipatuhi adalah termasuk yang berikut: a. Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang formal; b. Mengkaji semula dan menguji aplikasi kritikal semasa melaksanakan perubahan ke atas	CTM dan Pengurus ICT

	sistem yang sedang beroperasi untuk memastikan tiada impak negatif ke atas keselamatan atau operasi organisasi; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Menghalang sebarang peluang untuk membocorkan maklumat; dan e. Mengawal selia dan memantau pembangunan perisian oleh pembekal, pakar runding dan pihak- pihak lain yang berkepentingan.	
PKS-0080106	**Pengurusan Teknikal Keterdedahan (*Vulnerability)***	**Tindakan**
	Bertujuan memastikan pelaksanaan pengurusan teknikal vulnerability adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya. Pelaksanaan pengurusan teknikal *vulnerability* ini perlu juga dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah termasuk memperoleh maklumat teknikal *vulnerability* yang tepat pada masanyake atas sistem maklumat yang digunakan, menilai tahap pendedahan organisasi terhadap vulnerability tersebut dan mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pengurus ICT

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 – Pengurusan Pengendalian Insiden Keselamatan		
Objektif Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan, dan memastikan sistem ICT Kerajaan dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej jabatan dan sistem penyampaian perkhidmatan awam.		
PKS-0090101	**Insiden Keselamatan**	**Tindakan**
	Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. la mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Ketua Jabatan hendaklah melaksanakan tindakan ke atas insiden keselamatan ICT mengikut peraturan atau prosedur yang ditetapkan oleh Kerajaan dari semasa ke semasa.	Ketua Jabatan
PKS-0090102	**Mekanisme Pelaporan Insiden Keselamatan ICT**	**Tindakan**
	a. Pelaporan Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada Pegawai Keselamatan ICT (ICTSO) jabatan dan kepada Jabatan Pertahanan Awam Malaysia	ICTSO APM CERT GCERT

	Computer Emergency Response Team (APM CERT) atau kepada Government Computer Emergency Response Team (GCERT), untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak- pihak yang dibenarkan. b. Pelantikan Pegawai Bertanggungjawab Pegawai Keselamatan ICT jabatan dan anggota pasukan CERT jabatan mestilah dilantik secara rasmi oleh pengurusan jabatan masing-masing, dan semua warga jabatan berkenaan perlu maklum akan pelantikan pegawai-pegawai ini, dan perlu sentiasa bersedia untuk memberi respon apabila diperlukan. c. Tanggungjawab Pengguna Semua penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT, kerentanan yang diperhatikan atau disyaki terdapat dalam perkhidmatan dan sistem maklumat jabatan menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan pencerobohan.	

	d. 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 kepada jabatan- jabatan.	
PKS-0090103	**Prosedur Pengendalian Insiden Keselamatan ICT**	**Tindakan**
	Semua pegawai pasukan pengendali insiden keselamatan ICT iaitu anggota APM CERT perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard keselamatan ICT GCERT.	CTM dan Pengurus ICT
PKS-0090104	**Pengurusan Maklumat Insiden Keselamatan ICT**	**Tindakan**
	a. Perancangan Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan bagi mengawal kekerapan, kerosakan dan kos kejadian insiden akan datang, dan untuk tujuan mengkaji semula dasar-dasar keselamatan	CTM dan Pengurus ICT

	aset ICT sedia ada. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada jabatan. b. Bahan Bukti Jabatan hendaklah memastikan bahan-bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, diselenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan- bahan bukti seperti jejak audit, backup secara berkala, media backup offline ini hendaklah mengikut amalan terbaik yang disarankan oleh kerajaan dari semasa ke semasa. Jabatan juga hendaklah memastikan semua bahan bukti adalah selaras dengan peraturan pengumpulan maklumat dari segi kualiti, kelengkapan dan kebolehpercayaan bahan bukti yang termaktub dalam bidang kuasa perundangan berkenaan. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Melindungi integriti semua bahan bukti; b. Menjalinkan bahan bukti oleh personel yang dipertanggungjawabkan; c. Merekod semua maklumat aktiviti penyalinan termasuk pegawai terlibat, media, perisian, perkakasan dan tools yang digunakan;	

	d. Memaklumkan pihak berkuasa perundangan, seperti pegawai undang-undang dan polis (jika perlu); dan e. Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang diperlukan.	

PENGURUS KESINAMBUNGAN PERKHIDMATAN

1001 – Pengurus Kesinambungan Perkhidmatan		
Objektif Untuk memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
PKS-100101	**Pelan Kesinambungan Perkhidmatan**	**Tindakan**
	Pelan Kesinambungan Perkhidmatan hendaklah dibangunkan bagi menentukan pendekatan yang menyeluruh diambil mengekalkan kesinambungan perkhidmatan jabatan. Ini bertujuan memastikan tindakan pemulihan yang cekap dan berkesan dilaksanakan apabila berlakunya musibah atau bencana. Perkara-perkara berikutyang mesti dipatuhi termasuk berikut: **a. Perakuan Pengurusan** Pelan ini mestilah diperakukan oleh pengurusan jabatan. **b. Program Latihan Kesedaran** Program Latihan kesedaran kepada semua warga jabatan mengenai pelan ini dan proses serta prosedur yang terlibat perlu dilaksanakan **c. Penyelenggaraan Pelan** Pelan Kesinambungan Perkhidmatan perlu	Ketua Jabatan

	diselenggara secara berkala dan diuji pelaksanaannya terutama apabila terdapat perubahan dalam operasi dan sistem penyampaian perkhidmatan jabatan/ Kerajaan.	

PEMATUHAN

1101 – Pematuhan		
Objektif Untuk menghindar pelanggaran undang-undang jenayah dan sivil, *statutory*, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain		
PKS-110101	**Pematuhan Keperluan Perundangan**	**Tindakan**
	Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan bahawa pematuhan dan sebarang pelanggaran dielakkan.	
PKS-110102	**Pematuhan Dasar**	**Tindakan**
	Langkah-langkah perlu bagi mengelakkan sebarang pelanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Polisi Keselamatan Siber APM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa.	
PKS-110103	**Keperluan Perundangan**	**Tindakan**
	Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di jabatan termasuklah seperti berikut: a. Keselamatan perlindungan secara am 1. Emergency (Essential Power) Act 1964; 2. Essential (Key Points) regulations 1965; 3. Arahan Keselamatan yang	

	dikuatkuasakan melalui Surat Pekeliling Am Bil. 1 tahun 1985; 4. Arahan tetap Sasaran Penting yang dikeluarkan kepada pihak yang terlibat dalam pengurusan sasaran penting milik Kerajaan dan Swasta yang diluluskan oleh Jemaah Menteri pada 13 Oktober 1993; dan 5. Keselamatan Dokumen b. Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control); 1. Akta Rahsia Rasmi 1972; 2. Akta Arkib Negara 2003; 3. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta RasmiDan Penderiaan Jauh; 4. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (espionage); 5. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976; 6. Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987	

	Yang Ditandatangani Oleh Y.Bhg Ketua Setiausaha Negara Melalui Surat M(R)10308/3/(45) Bertarikh 8 Mei 1987; dan 7. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R)200/55 Klt.7(21) Bertarikh 21 Ogos 1999. c. Keselamatan Fizikal Bangunan; 1. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959; 2. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan; 3. State Key Points; 4. Surat Pekeliling Am Rahsia Bil. 1 Tahun 1975 - Keselamatan Jabatan-Jabatan Kerajaan; 5. Surat Bil. KPKK/308/A (2) bertarikh 7/9/79 - Mencetak Pas- Pas Keselamatan dan Kad-Kad Pengenalan Kementerian/ Jabatan; 6. Surat pekeliling Am Bil. 4 tahun 1982 – Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan 7. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka d. Keselamatan Individu	

	1. Government Security Officer: Terms of Reference - Extract On Training of Departmental Security Office Confidential; 2. General Circular Memorandum; 3. Instruction On Positive Vetting Procedure; 4. Surat Pekeliling Am Sulit Bil. 1/1966 - Perkara Keselamatan Tentang Persidangan-Persidangan/Perjumpaan Lawatan Sambil Belajar Antarabangsa; 5. Surat Pekeliling Tahun 1966 - Tapisan Keselamatan TerhadapPakar/Penasihat Luar Negeri; 6. Surat Pekeliling Am Sulit Bil. 1/1967 - Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka-mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam Perwakilan Rasmi Malaysia semasa melawat Negara-negara Tabir Buluh dan Tabir Besi; 7. Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 - Melaporkan Perjumpaan/ Percakapan Di Antara Diplomat/Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota-Anggota Kerajaan; dan 8. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Jabatan-Jabatan Kerajaan.	

	e. Keselamatan Aset ICT 1. Akta Tandatangan Digital 1997; 2. Akta Jenayah Komputer 1997; 3. Akta Hak Cipta (Pindaan) 1997; 4. Akta Multimedia dan Telekomunikasi 1998; 5. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan; 6. Pekeliling Am Bil. 3 Tahun 2000 - Rangka Dasar KeselamatanTeknologi Maklumat dan Komunikasi; 7. Pekeliling Am Bil. 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT); 8. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet & Mel Elektronik di Jabatan- Jabatan Kerajaan; 9. Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002; dan 10. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis PanduanMelaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005. f. Akta-akta dan Peraturan-peraturan lain yang berkaitan dengan APM 1. Akta 221 2. Akta Pertahanan Awam 1951 (Disemak 1979)	

	3. Kaedah-kaedah Pertahanan Awam (Bencana Diri) 1970 4. Kaedah-kaedah Pertahanan Awam (Pasukan Pertahanan Awam) 1970 5. Peraturan Pertahanan Awam (Pakai Seragam) 1983 6. Akta 425 7. Akta Perkhidmatan Negara 1952 (Semakan 1990) 8. Perlembagaan Malaysia - Jadual Kesembilan 9. Skim 'Non-Operational' Pertahanan Awam 10. Pelan Kontinjensi Kebangsaan Menghadapi Peperangan 11. Dasar Pertahanan Menyeluruh (HANRUH) 12. Arahan Menteri 13. Arahan Dan Pekeliling Jabatan 14. Deklarasi ICDO (International Civil Defence Organisation) 15. Arahan MKN (Majlis Keselamatan Negara)	
PKS-110104	**Pelanggaran Perundangan**	**Tindakan**
	Mengambil tindakan undang-undang dan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta-akta dan peraturan- peraturan lain yang berkaitan.	

BAHAGIAN : 03

GLOSARI

Active Directory (AD)	Teknologi Microsoft yang digunakan untuk mengurus komputer dan peralatan lain dalam rangkaian
Ancaman	Apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah
Antivirus	Perisian yang mengimbas virus pada media storan, seperti cakera keras (hardisk) dan disket (diskette) untuk sebarang kemungkinan adanya virus
Aplikasi	Perisian komputer atau program yang khusus digunakan untuk peranti mudah alih
Aset Alih	Aset atau peralatan yang boleh dipindahkan atau dialihkan dari satu tempat ke tempat lain secara mudah termasuk Aset Alih yang dibekalkan bersekali dengan penyediaan bangunan atau infrastruktur lain
Aset ICT	Aset ICT merangkumi perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia yang mempunyai nilai
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
Bilik khas	Bilik yang selamat dan terkawal
Business Resumption Plan	Pelan yang berupaya untuk meneruskan operasi jika berlaku gangguan perkhidmatan. Dalam situasi pelan sukar dilaksanakan sepenuhnya, maka pelan ini seboleh-bolehnya dapat melaksanakan fungsi-fungsi bagi operasi teras
CCTV	Closed-circuit television Sistem TV yang digunakan secara komersil di mana satu system TV kamera video dipasang dalam premis pejabat bagi tujuan membantu pemantauan fizikal

CDO	Chief Digital Officer Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan system maklumat bagi menyokong arah tuju sesebuah organisasi
Clear Desk	Tidak meninggalkan sebarang dokumen yang sensitif di atas meja
Clear Screen	Tidak memaparkan sebarang maklumat sensitif apabila komputer berkenaan ditinggalkan
Encryption	Enkripsi atau penyulitan. Proses enkripsi 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 peralatan atau perisian atau kombinasi kedua-duanya
ICT	Information and Communication Technology
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer
Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana computer 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
Insiden Keselamatan	Musibah (adverse event) yang berlaku ke atas sistem maklumat
Kriptografi	Satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja

LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer
Lock	Mengunci komputer
Log out	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer
Mobile Code	Kod perisian yang dipindakan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan Ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Penilaian Risiko	Penilaian ke atas kemungkinan berlakunya bahaya, kerosakan atau kehilangan aset
Penyulitan	Menjadikan teks biasa (plain text) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks cipher. Bagi mendapatkan semula teks biasa tersebut, proses penyahsulitan digunakan
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
Pemilik	Pegawai yang didaftarkan sebagai pemilik aset dan dipertanggungjawabkan ke atas aset tersebut
Pengguna	Pengguna terdiri daripada warga APM dan pihak luar yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT APM
Perisian	Program atau aturcara komputer yang dapat digunakan dengan sistem komputer tertentu

Perisian Aplikasi	Ia merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan
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 APM atas urusan rasmi
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 Malaysia
Restoration	Pemulihan ke atas data
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian internet.
Risiko	Kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian
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
Vulnerability	Sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER APM

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

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya berjanji bahawa saya akan mematuhi peruntukan Polisi Keselamatan Siber Angkatan Pertahanan Awam Malaysia serta apa-apa peraturan dan arahan lain yang berkaitan dikeluarkan dan dikuatkuasakan dari masa ke semasa selanjutnya tempoh perkhidmatan saya.
2. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub di dalam Dasar Keselamatan ICT Jabatan; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan dan disabitkan kerana melanggar Polisi Keselamatan Siber Jabatan, maka tindakan tatatertib boleh diambil ke atas diri saya mengikut Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib 1993).

.....
(Tanda Tangan Pegawai / Kakitangan)
Tarikh : .....

Disahkan Oleh :
Pegawai Keselamatan ICT (ICTSO)

.....
( )

Tarikh : .....

Diperakui Oleh :
Ketua Pegawai Maklumat (CIO)

.....
( )

Tarikh : .....