KEMENTERIAN PENGANGKUTAN
AGENSI PENGANGKUTAN AWAM DARAT

VERSI 1.0

POLISI KESELAMATAN SIBER

AGENSI PENGANGKUTAN AWAM DARAT
BAHAGIAN APLIKASI TEKNOLOGI

ISI KANDUNGAN

SEJARAH SEMAKAN DAN PINDAAN DOKUMEN

VERSI	TARIKH	KELULUSAN	TARIKH KUATKUASA	KETERANGAN PINDAAN
1.0	03 DIS 2024	Mesyuarat Jawatankuasa Pemandu ICT APAD Bil 2/2024 bertarikh 3 Dis 2024	04 DIS 2024	Menggantikan Dasar Keselamatan ICT (1 Sept 2020)

TUJUAN

Polisi Keselamatan Siber (PKS), Agensi Pengangkutan Awam Darat (APAD) ini bertujuan untuk **menerangkan mengenai tanggungjawab dan mengandungi peraturan-peraturan** yang perlu dibaca, difahami dan dipatuhi oleh warga APAD, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital ICT APAD dalam melindungi maklumat di ruang siber dan peranan dalam melindungi aset ICT dan keselamatan ICT APAD.

Ruang siber ditakrifkan sebagai sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT.

LATAR BELAKANG

Polisi ini dibangunkan untuk menjamin kesinambungan perkhidmatan APAD dengan meminimumkan kesan insiden keselamatan siber. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi APAD bagi memastikan semua maklumat dilindungi.

OBJEKTIF

Objektif utama Polisi Keselamatan ICT APAD adalah seperti berikut:

1) Menerangkan kepada semua pengguna merangkumi warga APAD, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital APAD mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber;
2) Memastikan keselamatan penyampaian perkhidmatan APAD di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak-pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;
3) Memastikan kesinambungan perkhidmatan dan kelancaran operasi APAD dengan meminimumkan kerosakan atau kemusnahan sekiranya berlaku insiden keselamatan yang tidak diingini;
4) Melindungi kepentingan pihak-pihak yang bergantungan kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

5) Mencegah salah guna atau kecurian aset ICT Kerajaan;
6) Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan siber dan pentadbiran ICT APAD;
7) Memastikan integriti dokumen dan maklumat elektronik adalah daripada sumber yang sah dan tanpa keraguan supaya sentiasa tepat, lengkap, sahih, terpelihara dan kemas kini. Ia hanya boleh diubah dengan kaedah yang dibenarkan;
8) Memastikan akses hanya kepada pengguna-pengguna yang sah;
9) Mencegah salah guna atau kecurian aset ICT Kerajaan; dan
10) Memberi kesedaran keselamatan ICT kepada warga APAD dan pemegang taruh.

ASET ICT APAD

Bagi menentukan **aset ICT** ini terjamin keselamatannya sepanjang masa, PKS APAD ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan dalam penghantaran dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ia merangkumi **Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran, Sumber Luaran, Manusia dan Tadbir Urus serta Premis Komputer dan Komunikasi.**

Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam menetapkan keperluan-keperluan asas dan pengendalian semua perkara-perkara berikut:

1) MAKLUMAT

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

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

(iii) Data dan maklumat juga adalah termasuk koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik yang mengandungi maklumat untuk digunakan bagi mencapai misi dan objektif agensi seperti sistem dokumentasi, prosedur operasi, rekod-rekod agensi, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain; dan

(iv) Semua penyedia perkhidmatan dalam APAD hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

a. Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), bermaksud Maklumat Rahsia Rasmi ialah 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 28 Akta Rahsia Rasmi 1972.

b. Maklumat Rasmi

Maklumat rasmi ialah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh APAD semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

c. Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (PII atau ***Personally Identifiable Information***) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

d. Data Terbuka

Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsi dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. Pll dikecualikan daripada data terbuka.

2) ALIRAN DATA

Aliran Data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi di APAD hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:

(i) Saluran komunikasi dan aliran data antara sistem di APAD;

(ii) Saluran komunikasi dan aliran data ke sistem luar; dan

(iii) Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

3) PLATFORM APLIKASI DAN PERISIAN

Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji secara berkala.

Perisian iaitu program, prosedur atau peraturan yang ditulis dan didokumentasikan yang berkaitan dengan sistem pengoperasian komputer yang disimpan 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 APAD;

4) PERANTI FIZIKAL DAN SISTEM

Semua platform fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji secara berkala. Ia merupakan aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan agensi. Peranti fizikal termasuk:

(i) Pelayan;

(ii) Peranti/Peralatan Rangkaian;

(iii) Workstation, Komputer Peribadi/Komputer Riba;

(iv) Telefon/peranti pintar;

(v) Media Storan;

(vi) Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);

(vii) Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan; dan

(viii) Peranti pengesahan (authentication devices), contohnya token keselamatan, dongle dan alat pengimbas biometrik.

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsi peranti fizikal dan sistem antaranya seperti berikut:

(i) Perkhidmatan rangkaian seperti LAN, WAN, Wireless dan lain-lain.

(ii) Sistem halangan akses seperti sistem kad akses.

(iii) Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

5) SISTEM LUARAN

Sistem luaran ialah sistem bukan milik APAD yang dihubungkan melalui sistem APAD. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

6) SUMBER LUARAN

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi APAD. Contoh perkhidmatan sumber luaran ialah:

(i) Perisian Sebagai Satu Perkhidmatan (Saas);

(ii) Platform Sebagai Satu Perkhidmatan (PaaS);

(iii) Infrastruktr Sebagai Satu Perkhidmatan (IaaS);

(iv) Storan Pengkomputeran Awan (Cloud Storage); dan

(v) Pemantauan Keselamatan.

7) MANUSIA ATAU TADBIR URUS

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

8) PREMIS KOMPUTER DAN KOMUNIKASI

Melibatkan kesemua kemudahan serta premis yang digunakan untuk menempatkan perkara (1) - (7) di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Semua saluran komunikasi dan aliran data kepada perkhidmatan hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

RISIKO

APAD hendaklah mengenal pasti kewujudan risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian sesuatu kecelakaan atau bencana berlaku yang menyebabkan kerosakan sehingga terjejas fungsi perkhidmatan sesuatu jabatan. Justeru itu APAD perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas risiko keselamatan aset dan keselamatan maklumat ICT.

Penilaian risiko hendaklah dilaksanakan secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber APAD. Penilaian risiko hendaklah dilaksanakan ke atas sistem maklumat termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

1) 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.

2) Ancaman (*Threat*)

APAD hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

3) Impak (*Impact*)

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

4) Tahap Risiko

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

5) Penguraian Risiko

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

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

a. Teknologi

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

b. Proses

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

c. Manusia

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

6) Pengurusan Risiko

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

(i) Mengenal pasti kerentanan;

(ii) Mengenal pasti ancaman;

(iii) Menilai risiko;

(iv) Menentukan penguraian risiko;

(v) Memantau keberkesanan penguraian risiko; dan

(vi) Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

APAD bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024.

APAD perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(i) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

(ii) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;

(iii) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

(iv) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

PRINSIP-PRINSIP KESELAMATAN

Prinsip-prinsip hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, prinsip-prinsip yang menjadi asas kepada PKS APAD dan perlu dipatuhi adalah seperti berikut:

1) Akses Atas Dasar (Prinsip Perlu Tahu)

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

2) Hak Akses Minimum (*Minimum previlege*)

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud,

menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

3) Kawalan Capaian Berdasarkan Peranan

Capaian sistem dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

4) Peminimuman Data

Menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

5) Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

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

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

(iii) Menentukan maklumat sedia untuk digunakan;

(iv) Menjaga kerahsiaan kata laluan;

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

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

(vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

6) Pengasingan Tugas

Setiap tugasan, proses dan persekitaran pelaksanaan ICT seperti wewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu dipisahkan dan diasingkan sebaik mungkin untuk mengekalkan integriti dan perlindungan keselamatan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi.

Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pembangunan, operasi dan rangkaian seperti berikut:

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

(ii) Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji; dan

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

7) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Pengauditan adalah penting dalam menjamin akauntabiliti seperti berikut:

(i) Mengesan pematuhan atau pelanggaran polisi keselamatan;

(ii) Menyediakan catatan peristiwa mengikut turutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran polisi keselamatan; dan

(iii) Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran polisi keselamatan.

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

8) Pematuhan

PKS APAD hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT melalui tindakan berikut:

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

(ii) Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;

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

(iv) Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

9) Pemulihan

Pemulihan amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan, mewujudkan dan menguji Pelan Pemulihan Bencana/Kesinambungan Perkhidmatan (DRC) serta melaksanakan amalan terbaik dalam pelaksanaan ICT; dan

10) Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan hendaklah dipatuhi bagi jaminan keselamatan yang berkesan. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin strategis mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

TEKNOLOGI

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

1) Peringkat Pemprosesan Data

(i) Data-dalam-simpanan (*data-at-rest*)

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

Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

(ii) Data-dalam-pergerakan (*data-in-motion*)

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

(iii) Data-dalam-penggunaan (*data-in-use*)

APAD hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

Teknologi yang bersesuaian boleh digunakan oleh APAD untuk memastikan asal data dan data/transaksi tanpa-sangkal.

(iv) Perlindungan ketirisan data (*data leakage protection*)

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

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

2) Elemen dalam persekitaran pengkomputeran

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

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputera mengikut Arahan Keselamatan yang dikeluarkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan daripada CGSO.

PROSES

Warga APAD hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

1) Konfigurasi asas

(i) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.

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

2) Kawalan perubahan konfigurasi

(i) Prosedur kawalan perubahan konfigurasi hendaklah diwujudkan dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem;

(ii) Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asa terkini; dan

(iii) Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

3) Sandaran

(i) Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.

(ii) Media sandaran hendaklah disimpan dalam persekitaran yang selamat da di peranti atau lokasi yang berasingan.

4) Kitaran pengurusan aset

(i) Pindah

Pemindahan hak milik aset berlaku dalam keadaan berikut:

a. Warga APAD meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan, penamatan kontrak atau penugasan semula;

b. Aset yang dikongsi untuk kegunaan sementara;

c. Pemberian aset kepada agensi lain; dan

d. Aset dikembalikan setelah tamat tempoh sewaan.

Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (ii).

(ii) Pelupusan

Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya;

Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A) 377. Peraturan-peraturan Arkib Negara (Penetapan Borang-borang bagi Pelupusan Rekod Awam) 2008.

Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data; dan
Sanitasi data hendaklah mengikut **Surat Pekeliling Am Bilangan 4 Tahun 2022 - Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.**

(iii) Kitaran hayat

Kitaran hayat data hendaklah diuruskan mengikut **Akta Arkib Negara 2003 (Akta 629);** dan

Akta Arkib Negara 2003 (Akta 629) memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umu selama lima tahun.

MANUSIA

Warga APAD, pembekal, pakar runding dan pihak-pihak kepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

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

1) Kompetensi pengguna

(i) Kompetensi pengguna termasuk:

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

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

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

2) Kompetensi pelaksana

(i) Warga APAD yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

(ii) Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

a. Mempunyai kelayakan akademi dalam bidang berkaitan atau sijil profesional keselamatan siber;

b. Memenuhi keperluan pembelajaran berterusan;

c. Menimba pengalaman yang mencukupi dalam bidang keselamatan siber; dan

d. Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

(iii) Pegawai Keselamatan ICT yang dilantik oleh APAD hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di APAD.

3) Peranan

(i) Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna;

(ii) Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani *Non-disclosure Agreement* (NDA) seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan;

(iii) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka;

(iv) Warga APAD yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Agensi dikembalikan sekiranya berlaku perubahan peranan;

(v) Warga APAD yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Agensi yang berkaitan seperti tersenarai dalam senarai aset Nota Serah Tugas; dan

(vi) Warga APAD lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Agensi dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Agensi.

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Setiap projek ICT yang dibangunkan di APAD hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

1) Peranti pengkomputeran peribadi

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

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

2) Peranti rangkaian

(i) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti VPN dan kabel.

(iii) 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

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

(ii) Teknologi dan kawalan keselamatan 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

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

(ii) 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

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

(ii) APAD hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

(iii) Pelindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip defence-in-depth.

(iv) 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.

PENYATAAN POLISI KESELAMATAN SIBER APAD

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

Keselamatan ICT adalah bermaksud keadaan 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 empat (4) komponen asas keselamatan ICT iaitu:

(i) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

(ii) Memastikan setiap maklumat adalah tepat dan sempurna;

(iii) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(iv) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

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

(i) Kerahsiaan – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

(ii) Integriti – Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(iii) Tidak Boleh Disangkal – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

(iv) Kesahihan – Data dan maklumat hendaklah dijamin kesahihannya; dan

(v) Ketersediaan – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

KAWALAN
01

POLISI KESELAMATAN MAKLUMAT

INFORMATION SECURITY POLICY

KAWALAN 01 – POLISI KESELAMATAN MAKLUMAT (*INFORMATION SECURITY POLICY*)

OBJEKTIF:

1) Untuk menjelaskan keperluan penggubalan dan pelaksanaan dasar-dasar berkaitan keselamatan maklumat dan keselamatan siber yang dinamakan Polisi Keselamatan Siber (PKS) APAD.

2) Penggubalan ini menggariskan hala tuju dan sokongan pihak pengurusan terhadap keselamatan maklumat selaras dengan keperluan APAD dan perundangan yang berkaitan selaras dengan tanggungjawab APAD sebagai peneraju perlindungan organisasi Infrastruktur Maklumat Kritikal Negara (CNII) bagi sektor pengangkutan.

KENYATAAN	TANGGUNGJAWAB
K01/01 – HALA TUJU PENGURUSAN UNTUK KESELAMATAN MAKLUMAT (*MANAGEMENT DIRECTIONS FOR INFORMATION SECURITY*)	
K01/01/01 – Polisi Keselamatan Maklumat (*Policies For Information Security*)	
K01/01/01/01 – Pelaksanaan Polisi	
Pelaksanaan polisi ini akan dijalankan oleh Ketua Pengarah APAD merangkap Ketua Pegawai Digital (CDO) yang bertanggungjawab dalam memastikan pelaksanaan PKS dengan cekap dan berkesan dibantu oleh Jawatankuasa yang setara dengannya (JPICT).	Ketua Jabatan dan JPICT
K01/01/01/02 – Penyebaran Polisi	
Dasar ini perlu disebarkan kepada semua pengguna APAD (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO
K01/01/01/03 – Pematuhan Polisi	
Polisi Keselamatan Siber APAD adalah terpakai kepada semua pengguna ICT APAD dan tiada pengecualian diberikan.	Warga APAD dan Pihak Ketiga

KENYATAAN	TANGGUNGJAWAB
K01/01/02 – Kajian Semula Polisi Untuk Keselamatan Maklumat (*Review Of Policies For Information Security*)	
K01/01/02/01 – Penyelenggaraan Polisi	
1) PKS APAD adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, polisi Kerajaan dan kepentingan sosial. 2) Berikut adalah prosedur penyelenggaraan PKS APAD: (i) Kenal pasti dan tentukan perubahan yang diperlukan; (ii) Kemukakan cadangan pindaan untuk dibentangkan dalam Mesyuarat JPICT APAD atau mesyuarat yang setara dengannya; (iii) Perubahan yang telah dipersetujui oleh JPICT APAD atau jawatankuasa yang setara dengannya dimaklumkan kepada warga APAD, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT APAD; dan (iv) Dasar ini hendaklah dikaji semula setiap LIMA (5) TAHUN SEKALI atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	ICTSO dan JPICT

KAWALAN
02

ORGANISASI KESELAMATAN MAKLUMAT

ORGANIZATION OF INFORMATION SECURITY

KAWALAN 02 – ORGANISASI KESELAMATAN MAKLUMAT

(*ORGANIZATION OF INFORMATION SECURITY*)

OBJEKTIF:

1) Menerangkan peranan dan tanggungjawab struktur tadbir urus individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber APAD.

2) Memastikan keselamatan telekerja dan penggunaan peralatan mudah alih.

KENYATAAN	TINDAKAN
K02/01 – PERANCANGAN DALAMAN *(INTERNAL ORGANIZATION)*	
K02/01/01 – Peranan Dan Tanggungjawab Keselamatan Maklumat (*The Role And Responsibility Of Information Security*)	
K02/01/01/01 – Ketua Pengarah / Ketua Pegawai Digital (CDO)	
1) Jawatan Ketua Pegawai Digital (CDO) APAD disandang oleh Ketua Pengarah APAD. 2) Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut: (v) Memastikan penguatkuasaan pelaksanaan Polisi ini; (vi) Memastikan warga APAD, pembekal, pakar runding dan pihak yang mempunyai urusan perkhidmatan digital APAD memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; (vii) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; (viii) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini; (ix) Mempengerusikan Mesyuarat JPICT APAD; dan (x) Melantik ICTSO	Ketua Pengarah/ CDO
K02/01/01/02 – Pengarah Bahagian Aplikasi Teknologi/Pengurus ICT APAD	
1) Jawatan Pengurus ICT APAD adalah disandang oleh Pengarah Bahagian Aplikasi Teknologi. 2) Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (i) Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;	Pengurus ICT APAD

KENYATAAN	TINDAKAN
(ii) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; (iii) Pembelian atau peningkatan perisian dan sistem komputer; (iv) Perolehan teknologi dan perkhidmatan teknologi baharu; (v) Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; (vi) Menentukan keperluan keselamatan ICT; (vii) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa; (viii) Memastikan setiap sistem yang dibangunkan telah dibuat ujian keselamatan; (ix) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan PKS APAD serta pengurusan risiko dan pengauditan; (x) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT APAD; (xi) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CDO APAD; dan (xii) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT APAD.	
K02/01/01/03 – Pegawai Keselamatan ICT (ICTSO)	
1) Jawatan ICTSO APAD adalah disandang oleh Ketua Penolong Pengarah (Gred F48). 2) Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (i) Merancang, mengurus dan melaksanakan program- program keselamatan dan kesedaran ICT APAD; (ii) Menguatkuasakan dan memantau pelaksanaan PKS APAD; (iii) Memberi penerangan dan pendedahan berkenaan PKS APAD kepada semua pengguna; (iv) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi APAD; (v) Menjalankan pengurusan risiko, audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/ garis panduan dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; (vi) Mengambil tindakan pembetulan ke atas hasil penemuan audit dan menyediakan laporan mengenainya;	ICTSO

KENYATAAN	TINDAKAN
(vii) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (viii) Melaporkan insiden keselamatan siber kepada Pasukan Tindak balas Insiden Keselamatan ICT (CSIRT) MOT, Pengurus ICT APAD dan Agensi Keselamatan Siber Negara (NACSA); (ix) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan melaksanakan langkah-langkah baik pulih dengan segera; (x) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; (xi) Koordinat Pelan Pengurusan Pemulihan Bencana (DR Koordinator) APAD; dan (xii) Melaporkan kes-kes pelanggaran PKS kepada Pengurus ICT APAD.	
K02/01/01/04 – Pentadbir Sistem ICT (Operasi)	
1) Pentadbir Sistem ICT (Operasi) APAD disandang oleh Pegawai Teknologi Maklumat (F41/F44). 2) Jawatan bertanggungjawab sebagai pentadbir rangkaian dan keselamatan, pentadbir pusat data dan pegawai aset. 3) Jawatan dibantu oleh Penolong Pegawai Teknologi Maklumat (FA32/FA29) dan Juruteknik Komputer (FT19). 4) Peranan dan tanggungjawab pentadbir sistem ICT (Operasi) adalah seperti berikut: (i) Pentadbir Rangkaian ICT a. Memastikan rangkaian setempat (LAN), rangkaian lua (WAN) dan Wireless beroperasi sepanjang masa; b. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; dan c. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian. (ii) Pentadbir Pusat Data	Pentadbir Rangkaian dan Keselamatan/ Pentadbir Pusat Data/ Pegawai Aset

KENYATAAN	TINDAKAN
a. Memastikan persekitaran fizikal, data dan sistem aplikasi berada dalam keadaan baik dan selamat; b. Menyediakan Pelan Pemulihan Bencana (DRP) bagi memastikan kesinambungan perkhidmatan; dan c. Memastikan pusat data sentiasa beroperasi mengikut polisi yang telah ditetapkan. (iii) Pegawai Aset a. Memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan; b. Merancang dan mengambil tindakan segera dari segi infrastruktur (emel/perkakasan) apabila kakitangan berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; c. Memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; d. Memastikan senarai aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ penaiktarafan aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira; e. Memastikan semua aset ICT Kerajaan yang disenaraikan mengandungi no siri peralatan, lokasi dan nama pemegang aset; f. Memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan bertulis daripada Ketua Jabatan/Bahagian; g. Memastikan setiap kerosakan aset ICT Kerajaan dilaporkan; h. Bertanggungjawab dalam menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan; i. Merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya sekali setahun; dan j. Memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur. (iv) Memastikan segala perubahan kepada polisi dan PKS dilaksanakan sekiranya memerlukan sebarang perubahan dan mendapat kelulusan JPICT APAD dan disebarkan semula kepada semua pengguna.	

KENYATAAN	TINDAKAN
K02/01/01/05 – Pentadbir Sistem ICT (Aplikasi)	
1) Pentadbir Sistem ICT APAD disandang oleh Pegawai Teknologi Maklumat (F41/F44). 2) Jawatan dibantu oleh Penolong Pegawai Teknologi Maklumat (FA32/FA29). 3) Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: (i) Pentadbir Sistem Aplikasi a. Mengambil tindakan segera berkaitan akses kepada aplikasi apabila dimaklumkan mengenai kakitangan berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini; c. Memantau aktiviti capaian harian pengguna; d. Mengenal pasti, memantau aktiviti-aktiviti pencerobohan dan pengubahsuaian data pada aplikasi tanpa kebenaran dan mengambil tindakan segera; e. Menyimpan dan menganalisis rekod jejak audit; f. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; dan g. Memastikan pembangunan sistem aplikasi yang dibangunkan mengambil kira dan mematuhi ciri-ciri keselamatan yang termaktub di dalam skop PKS APAD. (ii) Pentadbir Portal (*Webmaster*) a. Menerima kandungan portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b. Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; c. Memantau dan menganalisa log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka; d. Mengasingkan kandungan dan aplikasi dalam talian untuk capaian secara Intranet dan Internet ke portal APAD; e. Memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi;	Pentadbir Sistem Aplikasi/ Pentadbir Portal

KENYATAAN	TINDAKAN
f. Melaksanakan pengukuhan keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; g. Memantau proses *backup* dan *restoration* ke atas kandungan dan aplikasi portal; dan h. Melaporkan sebarang pelanggaran keselamatan portal kepada ICTSO.	
K02/01/01/06 – Jawatankuasa Pemandu ICT (JPICT)	
1) Jawatankuasa Pemandu ICT APAD (JPICT) adalah jawatankuasa yang bertanggungjawab untuk menilai, meluluskan serta menyokong aspek teknikal bagi keperluan dan keselamatan ICT APAD. 2) JPICT dipengerusikan oleh Ketua Pengarah merangkap CDO dengan keahlian terdiri daripada semua Pengarah Bahagian yang dilantik dan diurus setia oleh BAT. 3) Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil 3 Tahun 2015 ialah merancang dan menentukan langkah-langkah keselamatan siber. 4) Bidang kuasa JPICT berkaitan dengan keselamatan siber adalah: (i) Memperakukan, meluluskan dan menguatkuasakan dasar, hala tuju, garis panduan dan standard keselamatan ICT; (ii) Memantau tahap pematuhan keselamatan ICT; (iii) Memastikan PKS APAD selaras dengan dasar-dasar ICT semasa kerajaan; (iv) Menerima dan membincangkan laporan mengenai insiden-insiden keselamatan ICT semasa; (v) Membincang tindakan yang melibatkan pelanggaran PKS APAD; (vi) Meneliti dan meluluskan semua program dan aktiviti yang berkaitan dengan keselamatan ICT; (vii) Memastikan peruntukan kewangan yang mencukupi disediakan untuk pelaksanaan program dan aktiviti keselamatan.	JPICT
K02/01/01/07 – Pasukan Tindak Balas Insiden Keselamatan ICT Agensi (CSIRT APAD)	
1) Sebarang insiden keselamatan siber yang berlaku hendaklah dilaporkan terus kepada CSIRT di peringkat Kementerian Pengangkutan dan NACSA. 2) Maklumat berkaitan keanggotaan CSIRT APAD adalah seperti berikut: **Keahlian CSIRT di Peringkat Agensi** **Pengarah** : CDO APAD / Pengurus IT APAD **Pengurus** : ICTSO APAD	JPICT/Pengurus ICT/ICTSO/Pentadbir Sistem

KENYATAAN	TINDAKAN
Ahli : ✓ Pegawai Teknologi Maklumat di Jabatan ✓ Penolong Pegawai Teknologi Maklumat di Jabatan **Urus setia:** Bahagian/Unit/Seksyen IT 3) Peranan dan tanggungjawab CSIRT adalah seperti berikut: (i) Menerima dan merekodkan aduan keselamatan siber dan menilai tahap dan jenis insiden; (ii) Merekodkan dan menjalankan siasatan awal insiden yang diterima; (iii) Menangani tindak balas (response) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; (iv) Menghubungi dan melaporkan insiden yang berlaku kepada Agensi Keselamatan Siber Negara (NASCA) dan MOT sama ada sebagai input atau untuk tindakan seterusnya; (v) Menasihati Agensi/Bahagian/Perkhidmatan supaya mengambil tindakan pemulihan dan pengukuhan; (vi) Menyebarkan sebarang ancaman dan insiden keselamatan ICT serta makluman berkaitan pengukuhan keselamatan ICT kepada pengguna Agensi/Bahagian/Perkhidmatan; dan (vii) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
K02/01/01/08 – Pengguna	
1) Penjawat awam yang bekerja dan menggunakan rangkaian, aset dan sistem ICT di mana-mana Pejabat APAD. 2) Peranan dan tanggungjawab adalah seperti berikut: (i) Membaca, memahami dan mematuhi Polisi ini; (ii) Mengetahui dan memahami kesan tindakannya terhadap keselamatan ICT; (iii) Menjalani tapisan keselamatan seperti yang diarahkan (sekiranya diperlukan/dikehendaki berurusan dengan maklumat rasmi terperingkat atau yang berkaitan); (iv) Melaksanakan dan mematuhi prinsip-prinsip PKS APAD dan menjaga kerahsiaan maklumat Kerajaan/Agensi; (v) Melaksanakan langkah-langkah perlindungan berikut: a. Menjaga kerahsiaan maklumat APAD;	Warga APAD

KENYATAAN	TINDAKAN
b. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Pengurus ICT/ICTSO dengan segera; c. Menjaga kerahsiaan kata laluan atau kerahsiaan kawalan keselamatan siber dari diketahui umum; d. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; dan e. Mengendalikan maklumat terperingkat mengikut proses dan prosedur yang ditetapkan. (vi) Menghadiri program-program kesedaran mengenai keselamatan siber; (vii) Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini dan **menandatangani "Surat Akuan Pematuhan Polisi Keselamatan Siber Agensi Pengangkutan Awam Darat" (Lampiran 1)** bagi mematuhi Polisi ini; (viii) Tidak memasang sebarang perisian yang tidak sah dan tanpa kebenaran di perkakasan ICT APAD yang dibekalkan; (ix) Sebarang pertukaran keluar masuk APAD **MESTI** dimaklumkan dan mengikuti tatacara yang ditetapkan dari semasa ke semasa; (x) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT APAD dengan segera; dan (xi) Tidak menjejaskan imej Kerajaan dan bercanggah dengan dasar Kerajaan semasa.	
K02/01/01/09 – Pihak Ketiga - Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
1) Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. 2) Perkara yang perlu dipatuhi termasuk yang berikut: (i) Membaca, memahami dan mematuhi Polisi Keselamatan Siber APAD; (ii) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (iii) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (iv) Akses kepada aset ICT Agensi perlu berlandaskan kepada perjanjian kontrak; (v) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara yang perlu dimasukkan dalam perjanjian hendaklah selaras dengan :	CDO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga

KENYATAAN	TINDAKAN
a. Polisi Keselamatan Siber APAD; b. Arahan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972 (terkini); dan d. Hak Harta Intelek. (vi) **Menandatangani "Non Disclosure Agreement (NDA)" (Lampiran 2)** bagi mematuhi Polisi ini; (vii) Perkara yang perlu dipatuhi dalam berurusan dengan pembekal adalah seperti berikut: a. Mengenal pasti risiko keselamatan aset ICT serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; b. Capaian kepada aset ICT APAD perlu dinyatakan secara jelas dalam perjanjian perkhidmatan; dan c. Memantau pelaksanaan tugas oleh pembekal supaya mematuhi perjanjian perkhidmatan berkaitan keselamatan ICT.	
K02/02 – PERANTI MUDAH ALIH DAN TELEKERJA (*MOBILE DEVICES AND TELEWORKING*)	
K02/02/01 – Polisi Peranti Mudah Alih (Mobile Device Policy)	
1) Membangunkan serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih; dan 2) Meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga APAD.	JPICT dan BAT
K02/02/02 – Peranti Mudah Alih Milik Persendirian	
1) Peranti mudah alih milik persendirian hendaklah dikawal daripada mencapai maklumat Rahsia Rasmi dan hendaklah mematuhi polisi serta prosedur yang ditetapkan untuk dibawa masuk ke kawasan terperingkat; 2) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; 3) Peralatan mudah alih disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; 4) Tindakan perlindungan diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan;	Warga APAD

KENYATAAN	TINDAKAN
5) Peralatan mudah alih hendaklah dipasang dengan perisian keselamatan (antivirus, antimalware); dan 6) Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja.	
K02/02/03 – Telekerja (*Teleworking*)	
1) Telekerja meliputi semua bentuk pelaksanaan melaksanakan tugasan pejabat bukan dari Lokasi Pejabat; dan 2) Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja.	Warga APAD

KAWALAN
03

KESELAMATAN SUMBER MANUSIA

HUMAN RESOURCES SECURITY

KAWALAN 03 – KESELAMATAN SUMBER MANUSIA (HUMAN RESOURCES SECURITY)

OBJEKTIF:

1) Memastikan semua sumber manusia yang terlibat iaitu warga APAD, pembekal, pakar runding dan pihak-pihak yang berkepentingan yang mengakses dan menggunakan perkhidmatan digital APAD memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

2) Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

3) Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas diurus dengan teratur.

KENYATAAN	TINDAKAN
K03/01 – SEBELUM PERKHIDMATAN *(PRIOR TO EMPLOYMENT)*	
1) Tapisan keselamatan hendaklah dijalankan terhadap warga APAD, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital APAD yang terlibat selaras dengan keperluan perkhidmatan; 2) Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (i) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga APAD dan pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (ii) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan APAD serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan tatacara terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (iii) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani.	Pengurusan Sumber Manusia, Warga APAD dan Pihak Ketiga

KENYATAAN	TINDAKAN
K03/02 – DALAM TEMPOH PERKHIDMATAN (DURING EMPLOYMENT)	
1) Pihak pengurusan hendaklah memastikan warga APAD, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital APAD supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan. 2) Memastikan pihak yang terlibat dengan Maklumat Rahsia Rasmi hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan. 3) Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (i) Memberi latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberikan kepada pengguna ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (ii) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat; (iii) Memastikan adanya proses tindakan disiplin dan/atau undang-undang sekiranya perlu ke atas semua pengguna, pembekal, pakar runding dan pihak ketiga yang berkepentingan apabila berlaku perlanggaran dengan perundangan dan peraturan ditetapkan; dan (iv) Warga APAD yang melanggar polisi ini dan didapati bersalah akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT APAD.	Pengurusan Sumber Manusia dan Warga APAD
K03/03 – PENAMATAN DAN PERTUKARAN PERKHIDMATAN *(TERMINATION AND CHANGE OF EMPLOYMENT)*	
1) Warga yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut: (i) Memastikan semua aset ICT dikembalikan kepada BAT/ Pegawai Aset mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (ii) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan dan terma perkhidmatan yang ditetapkan; dan (iii) Maklumat rasmi kerajaan dalam peranti tidak dibenarkan dibawa keluar dari premis APAD tanpa kebenaran.	Pengurusan Sumber Manusia dan Warga APAD

KENYATAAN	TINDAKAN
2) Warga yang telah bertukar ke perkhidmatan/agensi lain hendaklah: (i) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada BAT/ Pegawai Aset mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (ii) Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	

KAWALAN

04

PENGURUSAN ASET

ASSET MANAGEMENT

KAWALAN 04 – PENGURUSAN ASET (*ASSET MANAGEMENT*)

OBJEKTIF:

1) Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT APAD.

2) Memastikan setiap aset dikenal pasti, dikelas, direkod dan di selenggara untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT.

3) Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

KENYATAAN	TINDAKAN
K04/01 – TANGGUNGJAWAB TERHADAP ASET *(RESPONSIBILITY FOR ASSETS)*	
K04/01/01 – Inventori Dan Pemilikan Aset ICT	
1) Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Aset-aset ICT APAD hendaklah diuruskan mengikut Tatacara Pengurusan Aset yang berkuatkuasa. 2) Aset yang boleh diselenggara hanyalah aset hak milik APAD. 3) Pentadbir aset ICT bertanggungjawab untuk menentukan prosedur kawalan khas (contohnya: kawalan capaian), kaedah pelaksanaan dan penyelenggaraan serta menyediakan langkah pemulihan yang konsisten dengan arahan pemilik aset. 4) Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: (i) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkodkan dalam borang daftar harta modal dan inventori perlu sentiasa dikemas kini; (ii) Memastikan aset telah dikelaskan dan dilindungi dimana pemilik aset perlu menentukan klasifikasi keselamatan yang bersesuaian bagi setiap maklumat aset; (iii) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (iv) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan APAD;	Pentadbir ICT, Pegawai Aset dan Warga APAD

KENYATAAN	TINDAKAN
(v) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan (vi) Setiap pengguna mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh pemilik aset atau pentadbir sistem dan perlu bertanggungjawab ke atas aset ICT di bawah tanggungannya sepenuhnya; (vii) Kehilangan atau kecurian aset ICT mestilah dilaporkan serta merta mengikut prosedur pengurusan kehilangan atau kecurian aset berpandukan Garis Panduan ICT APAD yang telah ditetapkan; (viii) Memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak; dan (ix) Memastikan semua jenis aset dipelihara dengan baik.	
K04/01/02 – Peralatan Mudah Alih Dan Kerja Jarak Jauh	
1) Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti berikut: (i) Memastikan bahawa tindkaan keselamatan yang bersesuaian diambil kira untuk dilindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; (ii) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; (iii) Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT; (iv) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan (v) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Pentadbir ICT, Pegawai Aset dan Warga APAD
K04/01/03 – Peminjaman Dan Pemulangan Aset ICT	
1) Perkara yang perlu dipatuhi dan diambil bagi **Peminjaman** adalah seperti berikut: (i) Melaksanakan permohonan peminjaman dengan justifikasi keperluan kepada Bahagian Aplikasi Teknologi; (ii) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh Agensi bagi membawa keluar peralatan bagi tujuan yang dibenarkan; (iii) Melindungi dan mengawal peralatan sepanjang masa;	Pentadbir ICT, Pegawai Aset dan Warga APAD

KENYATAAN	TINDAKAN
(iv) Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan (v) Menyemak peralatan ketika peminjaman dan pemulangan dilakukan. 2) Perkara yang perlu dipatuhi dan diambil bagi **Pemulangan** adalah seperti berikut: (i) Memastikan semua aset ICT dikembalikan kepada Agensi 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. (ii) Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.	
K04/02 – PENGELASAN MAKLUMAT (*CLASSIFICATION OF INFORMATION*)	
K04/02/01 – Pengelasan Maklumat	
1) Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh Pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. 2) Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (i) Rahsia Rasmi (ii) Rahsia Besar; (iii) Rahsia; (iv) Sulit; (v) Terhad; (vi) Dokumen Rasmi; dan (vii) Data terbuka	Pegawai Pengelas (Pentadbiran) Dokumen rasmi dan data terbuka dirujuk kepada PKS JDN
K04/02/02 – Pelabelan Dan Pengendalian Maklumat	
1) Semua maklumat mestilah dilabelkan mengikut klasifikasi maklumat seperti yang dinyatakan. 2) Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut : (i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;	Pegawai Pengelas dan Warga APAD

KENYATAAN	TINDAKAN
(ii) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (iii) Menentukan maklumat sedia untuk digunakan; (iv) Menjaga kerahsiaan kata laluan; (v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (vi) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; (vii) Memastikan maklumat terperingkat yang disimpan di dalam storan dalaman atau luaran (internal atau external hardisk) diberi pelindungan melalui kaedah enkripsi yang bersesuaian; dan (viii) Menjaga kerahsiaan langkah-langkah keselamatan ict dari diketahui umum.	
K04/03 – PENGENDALIAN MEDIA PENYIMPANAN MAKLUMAT (*MEDIA HANDLING*)	
K04/03/01 – Pengurusan Media Boleh Alih (*Management Of Removal Media*)	
1) Memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan aset secara tidak sah dan yang boleh mengganggu aktiviti perkhidmatan; 2) Prosedur perlu disediakan untuk pengurusan peralatan penyimpanan maklumat mudah alih mengikut pengkelasan yang telah ditetapkan di dalam dokumen Arahan Keselamatan; 3) Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (i) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (ii) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (iii) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (iv) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelakkan daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (v) Menyimpan semua jenis media di tempat yang selamat.	Pentadbir ICT, Pegawai Aset dan Warga APAD
K04/03/02 – Pelupusan Media (*Disposal Of Media*)	
1) Peralatan penyimpanan maklumat yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan.	Pentadbir ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.

KENYATAAN	TINDAKAN
2) Pelupusan media perlu mendapatkan kelulusan dan mengikut kaedah pelupusan ICT yang ditetapkan oleh Kerajaan. 3) Media yang mengandungi maklumat terperingkat hendaklah disanitasi terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	
K04/03/03 – Pemindahan Media	
1) Polisi, prosedur dan kawalan pertukaran maklumat yang rasmi perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi dalam Agensi dan mana-mana pihak terjamin. 2) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara Agensi dengan pihak luar. 3) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa dipindahkan keluar dari Agensi. 4) Perkara-perkara berikut perlu dipertimbangkan semasa pemindahan dilakukan seperti berikut: (i) Perkhidmatan pengangkutan atau kurier yang boleh dipercayai digunakan; (ii) Senarai kurier yang digunakan perlu mendapat persetujuan Ketua Jabatan; (iii) Pembungkusan perlu mencukupi bagi melindungi kerosakan fizikal yang mungkin timbul semasa transit; dan (iv) Rekod atau log perlu disimpan untuk mengenalpasti kandungan media, perlindungan yang digunakan serta rakaman semasa pemindahan kepada penjaga transit dan penerimaan di destinasi. 5) Pemindahan dokumen terperingkat secara fizikal perlu mengikut prosedur-prosedur seperti di Arahan Keselamatan.	Pentadbir ICT, Pegawai Aset dan Warga APAD

KAWALAN
05

KAWALAN AKSES

ACCESS CONTROL

KAWALAN 05 – KAWALAN AKSES (ACCESS CONTROL)

OBJEKTIF:

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

2) Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.

3) Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi serta perkhidmatan rangkaian.

4) Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.

5) Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

6) Memastikan keselamatan maklumat semasa menggunakan peralatan BYOD di APAD.

KENYATAAN	TINDAKAN
K05/01 – KEPERLUAN KAWALAN AKSES (*BUSINESS REQUIREMENTS OF ACCESS CONTROL*)	
K05/01/01 – Polisi Kawalan Akses	
1) Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. 2) Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Ia perlu direkodkan, dikemas kini mengikut keperluan semasa dan menyokong dasar kawalan capaian pengguna sedia ada. 3) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (ii) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;	CDO, Pengurus ICT, ICTSO dan Pentadbir ICT

KENYATAAN	TINDAKAN
(iii) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; (iv) Kawalan ke atas kemudahan pemprosesan maklumat; (v) Keperluan keselamatan aplikasi; (vi) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; (vii) Keperluan semakan hak akses berkala; (viii) Pembatalan hak akses; (ix) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan Keistimewaan akses (*access privilege*).	
K05/01/02 – Capaian Kepada Rangkaian Dan Perkhidmatan Rangkaian (*Access To Networks And Network Services*)	
1) Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari Pentadbir Rangkaian APAD. 2) Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (i) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian APAD, rangkaian agensi lain dan rangkaian awam; (ii) Mewujud dan menguatkuasakan mekanisme pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan (iii) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Pengarah Bahagian dan Pentadbir ICT
K05/02 – PENGURUSAN AKSES PENGGUNA	
K05/02/01 – Akaun Pengguna (Pendaftaran Dan Pembatalan Pengguna)	
1) Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. 2) Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: (i) Akaun yang diperuntukkan oleh APAD sahaja boleh digunakan; (ii) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (iii) Akaun pengguna yang diwujudkan pertama kali akan diberi hak capaian (access right) paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang	Pentadbir ICT dan Warga APAD

KENYATAAN	TINDAKAN
perubahan hak capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (iv) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan APAD. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (v) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (vi) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna berdasarkan kelulusan yang diterima dari pemilik proses atas sebab-sebab berikut; a. Pengguna dari Kumpulan Sokongan yang bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan; b. Bertukar bidang tugas kerja; c. Bertukar ke agensi lain; d. Bersara; atau e. Ditamatkan perkhidmatan.	
K05/02/02 – Hak Capaian Pengguna (*User Access*)	
1) Proses formal peruntukan akses pengguna perlu dilaksanakan dalam pemberian atau pembatalan hak akses kepada semua jenis pengguna termasuk sistem dan perkhidmatan. 2) Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas dan perlu merangkumi seperti berikut: (i) Mendapatkan kebenaran daripada pemilik sistem atau perkhidmatan ICT; (ii) Menentusahkan tahap akses yang diberikan adalah wajar dan selaras dengan keperluan tugas; (iii) Memastikan hak akses tidak diaktifkan sebelum prosedur kebenaran dilengkapkan; (iv) Mengekalkan rekod berpusat untu khak akses yang diberikan kepada ID Pengguna; (v) Menyesuaikan hak akses pengguna yang menukar peranan atau pekerjaan dan segera menyekat atau menghapuskan hak akses pengguna yang telah meninggalkan organisasi; (vi) Mengkaji semula secara berkala hak akses tersebut.	Pentadbir ICT dan Warga APAD

KENYATAAN	TINDAKAN
K05/02/03 – Pengurusan Kata Laluan	
1) 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 APAD seperti berikut: (i) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (ii) Membenarkan pengguna menukar kata laluan sendiri; (iii) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi; (iv) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf, simbol dan nombor (Alphanumerik); (v) Kata laluan hendaklah diingat dan **TIDAK BOLEH** didedahkan dengan apa cara sekalipun; (vi) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (vii) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; (viii) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas kata laluan diset semula; (ix) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (x) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; dan (xi) Kata laluan hendaklah ditukar selepas tempoh 90 hari atau sekurang-kurangnya setiap tiga (3) bulan atau selepas tempoh masa bersesuaian.	ICTSO, Pemilik Projek, Pentadbir ICT dan Warga APAD
K05/03 – KAWALAN CAPAIAN RANGKAIAN	
K05/03/01 – Capaian Rangkaian	
1) Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (i) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian APAD, rangkaian agensi lain dan rangkaian awam; (ii) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (iii) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO dan Pentadbir ICT

KENYATAAN	TINDAKAN
K05/03/02 – Capaian Internet	
1) Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (i) Penggunaan Internet di APAD hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian 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 APAD; (ii) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; (iii) Kaedah Content Filtering mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (iv) Penggunaan teknologi packet shaper untuk mengawal aktiviti (video conferencing, video streaming, chat, downloading) adalah perlu bagi menguruskan penggunaan bandwidth yang maksimum dan lebih berkesan; (v) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh pegawai yang diberi kuasa; (vi) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; (vii) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; (viii) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh APAD; (ix) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti newsgroup dan bulletin board. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CDO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; (x) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali kecuali dengan kebenaran khas; dan (xi) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: a. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan	ICTSO dan Pentadbir ICT

KENYATAAN	TINDAKAN
b. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah dan subversif.	
K05/03/03 – Capaian Jarak Jauh	
1) Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (i) Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah Remote Access mestilah menggunakan kaedah penyulitan (encryption); (ii) Lokasi bagi akses ke sistem ICT APAD hendaklah dipastikan selamat; dan (iii) Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada CDO/Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Pentadbir ICT dan Warga APAD
K05/04 – KAWALAN CAPAIAN SISTEM DAN APLIKASI	
K05/04/01 – Kawalan Capaian Sistem Pengoperasian	
1) Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. 2) Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: (i) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (ii) Merekodkan capaian yang berjaya dan gagal. 3) Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (i) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Agensi; (ii) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; dan (iii) Menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. 4) Perkara-perkara yang perlu dipatuhi termasuk berikut: (i) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; (ii) mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (iii) mengehadkan dan mengawal penggunaan program; dan	Pentadbir ICT

KENYATAAN	TINDAKAN
(iv) mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
K05/04/02 – Capaian Sistem dan Aplikasi	
1) Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di APAD adalah terhad kepada pengguna dan tujuan yang dibenarkan. 2) Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: (i) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut hak capaian dan keselamatan maklumat yang telah ditentukan; (ii) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (iii) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (iv) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; (v) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan (vi) Sebarang maklumat yang perlu dimuat naik ke portal atau laman web hendaklah mendapat kebenaran daripada pegawai yang dipertanggungjawabkan. Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. 3) Kemudahan ini juga perlu bagi: (i) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (ii) Merekodkan capaian yang berjaya dan gagal. 4) Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (i) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Agensi; (ii) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; dan	Pentadbir ICT

KENYATAAN	TINDAKAN
(iii) Menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. 5) Perkara-perkara yang perlu dipatuhi termasuk berikut: (i) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; (ii) mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (iii) mengehadkan dan mengawal penggunaan program; dan (iv) mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
K05/04/03 – Peralatan Mudah Alih Dan Kerja Jarak Jauh (*Work From Home*)	
1) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. 2) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan. 3) Penggunaan talian luar seperti di premis luar adalah tidak digalakkan terutama melibatkan akses kepada maklumat sulit kerajaan.	Warga APAD
K05/04/04 – Keperluan Dan Kawalan Penggunaan *Bring Your Own Device* (BYOD)	
1) Penggunaan BYOD yang disambung kepada rangkaian APAD/MyGOVUC sama ada menyimpan atau mengakses data rasmi Kerajaan adalah tertakluk kepada perkara-perkara yang perlu dipatuhi seperti berikut: (i) Pengguna perlu mengetahui risiko dan kesan penggunaan BYOD terhadap keselamatan maklumat; (ii) Pengguna perlu mengetahui peraturan-peraturan yang telah ditetapkan apabila menggunakan BYOD; dan (iii) Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.	Warga APAD

KAWALAN
06

KRIPTOGRAFI

CRYPTOGRAPHY

KAWALAN 06 – KRIPTOGRAFI (CRYPTOGRAPHY)

OBJEKTIF:

1) Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, integriti, kesahihan dan keutuhan maklumat.

KENYATAAN	TINDAKAN
K06/01 – KAWALAN KRIPTOGRAFI (*CRYTOGRAPHY CONTROLS*)	
K06/01/01 – Dasar Kriptografi	
1) Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi yang termaktub di dalam buku arahan keselamatan pada setiap masa. 2) Kriptografi merangkumi kaedah-kaedah seperti yang berikut: (i) Peraturan bagi melindungi maklumat terperingkat menggunakan kaedah kriptografi yang sesuai dengan keperluan organisasi hendaklah diwujudkan dan dilaksanakan selaras dengan dasar dan peraturan yang berkuatkuasa; dan (ii) Keperluan kawalan kriptografi mestilah dinyatakan dalam semua perolehan dan pembangunan ICT baharu yang melibatkan maklumat terperingkat. Kaedah, kod sumber dan produk kriptografi yang digunakan mestilah boleh di akses oleh Kerajaan bagi tujuan kawalan, penialaian dan analisa keselamatan.	ICTSO, Pengurus ICT
K06/01/02 – Tandatangan Digital	
1) Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik bagi tujuan perlindungan kesahihan dan integriti. 2) Kemudahan tandatangan digital yang digunakan hendaklah mematuhi dasar dan peraturan yang berkuat kuasa.	Pentadbir ICT dan Warga APAD
K06/01/03 – Pengurusan Infrastruktur Kunci Awam (PKI)	
1) Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	ICTSO, Pentadbir Sistem dan Warga APAD

KENYATAAN	TINDAKAN
2) Perkara yang perlu dipatuhi adalah seperti berikut: (i) Penggunaan sijil digital hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; (ii) Sijil digital hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (iii) Perkongsian sijil digital untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; (iv) Sebarang perubahan kepada pemilik atau kehilangan/kerosakan hendaklah dilaporkan kepada pentadbir sistem. (v) Semua kunci kriptografi yang dihasilkan bagi melindungi maklumat terperingkat adalah hak milik Kerajaan; (vi) Kunci kriptografi mestilah diuruskan, diselia dan dilindungi dengan menggunakan kaedah yang ditetapkan dan hendaklah dirahsiakan; dan (vii) Semua kunci mestikan dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut.	

KAWALAN
07

KESELAMATAN FIZIKAL DAN PERSEKITARAN

PHYSICAL AND ENVIRONMENTAL SECURITY

KAWALAN 07 – KESELAMATAN FIZIKAL DAN PERSEKITARAN

(*PHYSICAL AND ENVIRONMENTAL SECURITY*)

OBJEKTIF:

1) Memastikan maklumat dan premis ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang bentuk pencerobohan, ancaman, bencana alam, kerosakan, kecuaian serta akses yang tidak dibenarkan.

2) Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.

3) Melindungi aset ICT dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

4) Melindungi maklumat dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

KENYATAAN	TINDAKAN
K07/01 – Keselamatan Kawasan (*Secure Areas*)	
K07/01/01 – Perimeter Keselamatan Fizikal (*Physical Security Parameter*)	
1) Perimeter keselamatan hendaklah ditakrifkan dan digunakan untuk melindungi Kawasan Larangan dan Tempat Larangan yang mengandungi maklumat sensitif atau kritikal dan juga kemudahan pemprosesan maklumat. 2) Ini bertujuan untuk menghalang akses tanpa kebenaran, kerosakan dan gangguan secara fizikal terhadap premis, aset ICT APAD dan maklumat agensi. 3) Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (i) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;	CDO, Pengurus ICT, ICTSO dan Bahagian Khidmat Pengurusan

KENYATAAN	TINDAKAN
(ii) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (iii) Memastikan alat penggera atau kamera (CCTV) sentiasa berfungsi dengan baik mengikut keperluan; (iv) Memastikan kaunter kawalan dan perkhidmatan keselamatan diwujudkan serta mengehadkan jalan keluar masuk bagi memastikan pengguna yang dibenarkan sahaja memasuki kawasan tersebut; (v) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; (vi) Mereka bentuk dan melaksanakan susun atur keselamatan fizikal di dalam ruang pejabat yang mempunyai kemudahan ICT; (vii) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana (force majeure); (viii) Menyediakan garis panduan (SOP) untuk pengguna yang bekerja di dalam kawasan terhad; (ix) Memastikan pihak yang dibenarkan sahaja memasuki kawasan terhad seperti kawasan penghantaran, pemunggahan dan juga lokasi lain yang dikenal pasti dari semasa ke semasa; dan (x) Sentiasa memastikan pihak ketiga yang membuat penyelenggaraan aset ICT diiringi.	
K07/01/02 – Kawalan Kemasukkan Fizikal	
1) Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis APAD. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: **(i) Warga APAD** a. Semua pegawai dan kakitangan APAD hendaklah memakai dan mempamerkan pas keselamatan sepanjang waktu bertugas; dan b. Pas keselamatan hendaklah dikembalikan kepada Unit Pentadbiran apabila pengguna bertukar, tamat perkhidmatan, bersara atau tamat kontrak. **(ii) Pelawat** a. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter kawalan keselamatan di pintu masuk pejabat APAD dan hendaklah dikembalikan semula selepas tamat lawatan. **(iii) Kehilangan Pas Keselamatan**	CDO, ICTSO, Bahagian Khidmat Pengurusan, Warga APAD, Pihak Ketiga dan Pelawat

KENYATAAN	TINDAKAN
a. Kehilangan pas mestilah dilaporkan dengan kadar segera kepada pejabat yang mengeluarkannya (Unit Pengurusan Pentadbiran, APAD) seperti yang ditetapkan.	
K07/01/03 – Kawasan Larangan	
1) Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. 2) Perkara-perkara yang perlu dipatuhi di kawasan larangan adalah seperti berikut: (i) Akses kepada kawasan larangan perlu dihadkan dan hanya diakses kepada pegawai-pegawai yang dibenarkan sahaja seperti bilik kawalan CCTV, bilik server dan bilik yang menempatkan perkakasan rangkaian; (ii) Sumber data, server, peralatan rangkaian dan komunikasi serta storan perlu ditempatkan di pusat data yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; (iii) Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai dan perlu diperiksa dan diselenggara secara berjadual; (iv) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; (v) Semua aktiviti pihak ketiga di kawasan larangan perlu mendapatkan kebenaran daripada pegawai yang diberi kuasa dan dipantau serta dikawal oleh pegawai bertanggungjawab dan direkodkan; (vi) Peralatan/media perakaman/storan/ komunikasi adalah tidak dibenarkan dibawa masuk ke dalam bilik server atau pusat data; (vii) Aktiviti mengambil gambar, merakam video, merekodkan suara atau penggunaan peralatan yang tidak berkenaan adalah dilarang; (viii) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi Arahan Keselamatan; dan (ix) Menghadkan jalan keluar masuk.	CDO, Pengurus ICT, ICTSO, Bahagian Khidmat Pengurusan, Warga APAD, Pihak Ketiga dan Pelawat

KENYATAAN	TINDAKAN
K07/02 – Keselamatan Peralatan	
K07/02/01 – Penempatan dan Perlindungan Peralatan ICT	
1) Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. 2) Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan dengan mengambil langkah-langkah keselamatan seperti berikut: (i) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (ii) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (iii) Pengguna dilarang sama sekali menambah, menanggalkan atau menukar ganti sebarang perkakasan ICT yang telah ditetapkan tanpa kebenaran; (iv) Pengguna dilarang membuat sebarang pemasangan (*installation*) perisian tanpa kebenaran Pentadbir Sistem atau pegawai yang dipertanggungjawabkan; (v) Pengguna mestilah memastikan perisian antivirus di komputer mereka dikemas kini dan sentiasa melakukan imbasan ke atas media storan yang digunakan; (vi) Semua peralatan sokongan ICT hendaklah dilindungi daripada dicuri, dirosakkan, disalah guna dan diubahsuai tanpa kebenaran; (vii) Setiap pengguna adalah bertanggungjawab ke atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; (viii) Peralatan-peralatan kritikal perlu dibekalkan dengan *Uninterruptable Power Supply* (UPS); (ix) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti switch, hub, router dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (x) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (xi) Peralatan ICT yang hendak dibawa keluar dari premis agensi, perlulah mendapat kelulusan dan direkodkan bagi tujuan pemantauan; (xii) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden berdasarkan garis panduan yang berkuatkuasa;	ICTSO, Pentadbir ICT dan Warga APAD

KENYATAAN	TINDAKAN
(xiii) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (xiv) Pengguna tidak dibenarkan memindahkan peralatan ICT dari tempat asal tanpa kebenaran pegawai yang dipertanggungjawabkan; (xv) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaikpulih; (xvi) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (xvii) Pengguna dilarang sama sekali mengubah katalaluan bagi akaun *administrator* yang telah ditetapkan oleh Pentadbir Sistem ICT; (xviii) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; dan (xix) Pengguna hendaklah mematikan semua suis perkakasan ICT dimatikan apabila meninggalkan pejabat bagi megelakkan kerosakan jika berlaku kejadian seperti petir, kilat dan sebagainya.	
K07/02/02 – Media Storan	
1) Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM dan media storan lain. 2) Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan. 3) Bagi menjamin keselamatan, perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (ii) Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu; (iii) Semua data di dalam media storan yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat; (iv) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;	ICTSO, Pentadbir ICT dan Warga APAD

KENYATAAN	TINDAKAN
(v) Media storan dan peralatan backup hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat; (vi) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; (vii) Media backup hendaklah diletakkan di tempat yang terkawal; dan (viii) Membuat salinan atau penduaan (data backup) bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.	
K07/02/03 – Media Tandatangan Digital	
1) Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut: (i) Pegawai hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (ii) Media ini tidak boleh dipindah-milik atau dipinjamkan; dan (iii) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO dan mengikut tatacara pengurusan aset alih kerajaan yang masih berkuatkuasa.	Pentadbir Sistem dan Pengguna
K07/02/04 – Media Perisian dan Aplikasi	
1) Sebarang perisian dan aplikasi yang digunakan hendaklah mematuhi perkara-perkara seperti berikut: (i) Hanya perisian yang sah sahaja dibenarkan bagi kegunaan APAD; (ii) Sebarang instalasi perisian selain daripada perisian pre-installed oleh BAT hendaklah mendapatkan kebenaran bertulis daripada CDO atau pegawai yang bertanggungjawab; (iii) Sistem aplikasi dalaman tidak dibenarkan diagih/didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (iv) 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 dan perlu disimpan di tempat yang selamat dan dikawal capaiannya; dan (v) Kod sumber (*source code*) sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Pengurus ICT, ICTSO, Pemilik Projek, Pentadbir ICT dan Warga APAD
K07/02/05 – Dasar Meja Kosong dan Skrin Kosong (*Clear Desk Dan Clear Screen*)	
1) Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.	Warga APAD

KENYATAAN	TINDAKAN
2) *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. 3) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; (ii) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (iii) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	
K07/02/06 – Peralatan di Luar Premis	
1) Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis APAD. 2) Perkakasan yang dibawa keluar dari premis adalah terdedah kepada pelbagai risiko. 3) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Peralatan perlu dilindungi dan dikawal sepanjang masa; (ii) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (iii) Keselamatan peralatan yang dibawa keluar adalah dibawah tanggungjawab pegawai yang berkenan.	Warga APAD
K07/02/07 – Penyelenggaraan Perkakasan	
1) Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti. 2) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Bertanggungjawab terhadap penyelenggaraan setiap perkakasan ICT sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (ii) Semua perkakasan yang di selenggara hendaklah mematuhi spesifikasi yang telah ditetapkan; (iii) Memastikan perkakasan hanya di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja;	CDO, ICTSO, Pengurus ICT, Pemilik Projek, Pentadbir ICT

KENYATAAN	TINDAKAN
(iv) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (v) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (vi) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT atau pegawai yang bertanggungjawab.	
K07/02/08 – Pelupusan Perkakasan	
1) Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (*overwrite*) sebelum dilupuskan atau diguna semula. 2) Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak ekonomik untuk dibaiki sama ada harta modal atau inventori yang dibekalkan. 3) Peralatan ICT yang hendak dilupuskan perlu mematuhi tatacara pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat yang terdapat di dalam aset ICT tidak terlepas dari kawalan. 4) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan atau disanitasi dengan cara yang selamat mengikut Arahan keselamatan dan tatacara Arkib Negara yang berkuatkuasa; (ii) Memastikan data-data dalam storan telah dihapuskan dengan cara yang selamat dan kekal sebelum peralatan ICT dilupuskan; (iii) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat salinan sandar; (iv) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (v) Peralatan yang hendak di lupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (vi) Pegawai aset bertanggungjawab merekodkan butir – butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem yang diguna pakai;	Pengurus ICT, Pegawai Aset dan Warga APAD

KENYATAAN	TINDAKAN
(vii) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; (viii) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:- a. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. b. Menanggalkan dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, Hardisk, Motherboard dan sebagainya; c. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di APAD; d. *Memindah* keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; e. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab APAD; dan (ix) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumbdrive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
K07/03 – Keselamatan Persekitaran	
K07/03/01 – Kawalan Persekitaran	
1) Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Bahagian Khidmat Pengurusan (BPK) APAD. 2) Bagi menjamin keselamatan persekitaran, perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; (ii) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;	CDO, Pengurusan ICT, ICTSO dan Bahagian Khidmat Pengurusan

KENYATAAN	TINDAKAN
(iii) Peralatan perlindungan (pemadam api, pengesan kebakaran dan sebagainya) hendaklah berfungsi dan diletakkan di tempat yang bersesuaian, mudah dicapai dan dikendalikan; (iv) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (v) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; (vi) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan (vii) Semua peralatan perlindungan keselamatan dan kebakaran hendaklah diselenggarakan mengikut jadual bagi memastikan ia dapat berfungsi dengan baik.	
K07/03/02 – Bekalan Kuasa	
1) Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. 2) Perkara-perkara yang perlu dipatuhi bagi memastikan keselamatan bekalan kuasa adalah seperti berikut: (i) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (ii) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan (iii) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa, diselenggara dan diuji secara berjadual oleh pihak penyelenggara bangunan.	CDO, Pengurusan ICT, ICTSO dan Bahagian Khidmat Pengurusan
K07/03/03 – Kabel Rangkaian	
1) Kabel rangkaian hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. 2) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Mendapatkan kelulusan daripada BKP dan BAT untuk sebarang pengubahsuaian; (ii) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* atau *tray* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; (iii) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;	ICTSO dan Pentadbir ICT

KENYATAAN	TINDAKAN
(iv) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (v) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan.	
K07/03/04- Prosedur Kecemasan	
1) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang sedang berkuatkuasa; dan (ii) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselanatan Kebakaran yang dilantik mengikut aras.	Warga APAD dan Pegawai Keselamatan Kebakaran
K07/03/05- Mekanisma Pelaporan Insiden Bukan ICT	
Semua pengguna yang terlibat haruslah melaporkan dan merekodkan sebarang kejadian atau kerosakan peralatan bukan ICT kepada pihak Bahahagian Khidmat Pengurusan.	Warga APAD dan Pegawai Keselamatan Kebakaran
K07/03/06- Mekanisma Kawalan Peralatan Ujicuba (*Proof of Concept (POC)*)	
1) Penerimaan (i) Peralatan yang diterima bebas daripada *virus*, *backdoor*, *worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT Agensi. 2) Penyelenggaraan (i) Capaian melalui rangkaian luar APAD adalah tidak dibenarkan; dan (ii) Aktiviti penyelenggaraan adalah di bawah pengawasan pegawai APAD. 3) Pemulangan (i) Maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*permanent delection*); dan (ii) Memastikan semua maklumat jabatan tidak tertinggal pada peralatan.	Pentadbir ICT
K07/04 – Keselamatan Sistem Dokumentasi	
K07/04/01 – Dokumen	
1) Bagi memastikan keselamatan sistem dokumentasi, perkara-perkara yang perlu dipatuhi selaras dengan akta, Arahan Keselamatan dan pekeliling yang sedang berkuat kuasa adalah seperti berikut: (i) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;	Warga APAD

KENYATAAN	TINDAKAN
(ii) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (iii) Pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (iv) Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	

KAWALAN
08

KESELAMATAN OPERASI

OPERATION SECURITY

KAWALAN 08 – KESELAMATAN OPERASI (*OPERATIONS SECURITY*)

OBJEKTIF:

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

2) Memastikan pengesanan aktiviti pemprosesan maklumat dan mencegah daripada kebocoran data secara tidak sah/tidak dibenarkan dan melindungi pengguna daripada menghantar maklumat sensitif atau maklumat penting keluar daripada rangkaian APAD bagi mengekalkan integriti maklumat dan perkhidmatan komunikasi.

3) Melindungi integriti maklumat agar boleh diakses pada bila-bila masa dan integriti perisian dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.

4) Meminimumkan risiko dan melindungi maklumat dalam rangkaian dan infrastruktur sokongan dan aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan yang menyebabkan gangguan atau kegagalan sistem.

5) Memastikan keselamatan pertukaran maklumat dan perisian dengan agensi luar terjamin disamping mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

KENYATAAN	TINDAKAN
K08/01 – Pengurusan Prosedur Operasi	
K08/01/01 – Pengendalian Dokumen Prosedur Operasi	
1) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Semua prosedur keselamatan ICT yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; (ii) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat,	Pengurus ICT, ICTSO, Pemilik Projek, Pentadbir ICT dan Pengguna

KENYATAAN	TINDAKAN
pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; (iii) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan; dan (iv) Memastikan pengguna mematuhi prosedur yang telah ditetapkan.	
K08/01/02 – Pengurusan Perubahan	
1) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (ii) Aktiviti-aktiviti seperti memasang, menyelenggarakan, 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; (iii) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan oleh pegawai atasan atau pemilik aset ICT; dan (iv) Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Pengurus ICT, ICTSO, Pemilik Projek, Pentadbir ICT dan Pengguna
K08/01/03 – Pengasingan Tugas dan Tanggungjawab	
1) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahan yang tidak dibenarkan ke atas aset ICT; (ii) Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan (iii) Perkakasan yang digunakan bagi tugas membangun, mengemas kini dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan dalam persekitaran pembangunan (*development*), pengujian (*testing*), persediaan (*staging*) dan persekitaran sebenar (*production*). Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian jika perlu.	ICTSO, Pemilik Projek dan Pentadbir ICT

KENYATAAN	TINDAKAN
K08/01/04 – Perkhidmatan Penyampaian Pihak Ketiga	
1) Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (i) Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pihak ketiga; (ii) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (iii) Pengurusan ke atas perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian risiko.	Pemilik Projek dan Pihak Ketiga
K08/02 – Perancangan dan Penerimaan Sistem	
K08/02/01 – Perancangan Kapasiti	
1) Bagi meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem, berikut adalah perkara yang perlu diambil kira: (i) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; (ii) Aset ICT EOL, EOS atau BER yang mendedahkan APAD kepada risiko keselamatan siber atau mengganggu perkhidmatan hendaklaj dikenal pasti dan dikawal bagi meminimumkan risiko; dan (iii) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	JPICT, Pengurus ICT, ICTSO, Pemilik Projek dan Pentadbir ICT
K08/02/02 – Penerimaan Sistem	
1) Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. 2) Satu surat pengesahan penerimaan hendaklah dikeluarkan dengan persetujuan kedua-dua pihak.	JPICT, Pemilik Sistem Pentadbir Sistem dan Pengguna

KENYATAAN	TINDAKAN
K08/03 – Perlindungan dari Perisian Berbahaya	
K08/03/01 – Perlindungan dari Perisian Berbahaya	
1) Perkara-perkara yang perlu dipatuhi untuk memastikan perlindungan aset ICT dari perisian berbahaya adalah seperti berikut: (i) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; (ii) Memasang dan menggunakan perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (iii) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya dan secara berkala; (iv) Mengemas kini antivirus dengan *pattern* antivirus yang terkini; (v) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (vi) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (vii) 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; (viii) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (ix) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus. 2) Penggunaan peranti luar atau *mobile code* seperti *usb, external hardisk* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pentadbir ICT dan Pengguna
K08/04 – Pencegahan Ketirisan Data (*Data Leakage Prevention*)	
K08/04/01 – Pencegahan Kebocoran Data	
1) Data di dalam sistem, rangkaian dan peralatan lain perlu dilindungi daripada pendedahan dan pengekstrakan data yang tidak sah oleh individu atau sistem. 2) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Mengenal pasti dan mengelas maklumat untuk di lindungi daripada ketirisan;	ICTSO, Pemilik Projek, Pentadbir ICT dan Penyelia Insiden

KENYATAAN	TINDAKAN
(ii) Memantau saluran transaksi dan perkongsian data contohnya mel elektronik, penghantaran fail, mobile services, media boleh alih; (iii) Melaksanakan tindakan pengukuhan untuk mengelakkan ketirisan maklumat; dan (iv) Melindungi data melalui pengurusan penggunaan, penghantaran dan penyimpanan.	
K08/05 – Housekeeping	
K08/05/01 – Sandaran (*Backup*)	
1) Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana atau insiden, *backup* seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. 2) Backup hendaklah direkodkan dan disimpan di *off site*, di antaranya adalah: (i) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (ii) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi mengikut prosedur yang telah ditetapkan. Kekerapan backup bergantung pada tahap kritikal maklumat; (iii) Menguji sistem backup dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (iv) APAD hendaklah menyimpan *backup* mengikut keperluan atau sekurang-kurangnya satu (1) generasi backup; dan (v) Merekodkan dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Pentadbir ICT dan Warga APAD
K08/06 – Pengurusan Media	
K08/06/01 – Media Storan Mudah Alih dan Prosedur Pengendalian Media	
1) Penghantaran atau pemindahan media storan mudah alih yang mengandungi maklumat terperingkat ke luar pejabat hendaklah mendapat kebenaran daripada Pengurusa ICT terlebih dahulu. 2) Di antara prosedur-prosedur pengendalian media termasuk: (i) Melabelkan semua media mengikut tahap keselamatan sesuatu maklumat;	Pentadbir ICT dan Warga APAD

KENYATAAN	TINDAKAN
(ii) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (iii) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (iv) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (v) Menyimpan semua media di tempat yang selamat; dan (vi) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
K08/06/02 – Paparan Maklumat Umum	
1) Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (i) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (ii) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (iii) Memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan sebelum dimuat naik ke laman web.	Warga APAD
K08/07 – Pemantauan	
K08/07/01 – Pengauditan dan Forensik ICT	
1) ICTSO/Pasukan CSIRT APAD mestilah bertanggungjawab merekodkan dan memaklumkan kepada Pasukan dan CSIRT MOT perkara-perkara berikut: (i) Sebarang percubaan pencerobohan kepada sistem ICT APAD; (ii) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam , pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*) ancaman (*threats*) dan kehilangan fizikal (*physical loss*); (iii) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (iv) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (v) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (vi) Aktiviti instalasi dan penggunaan perisian yang membebankan bandwidth rangkaian;	CDO ,ICTSO, Pasukan CSIRT APAD

KENYATAAN	TINDAKAN
(vii) Aktiviti penyalahgunaan akaun e-mel; dan (viii) Aktiviti penukaran IP *address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem. 2) Langkah-langkah yang perlu diambil adalah seperti berikut: (i) CSIRT APAD akan menentukan prosedur pengumpulan bahan bukti yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan; (ii) Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; (iii) Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan; dan (iv) Semua proses dan hasil siasatan adalah SULIT.	
K08/07/02 – Jejak Audit	
1) Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekodkan aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. 2) Jejak audit hendaklah mengandungi ciri-ciri berikut: (i) Rekod setiap aktiviti transaksi; (ii) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (iii) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (iv) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. 3) Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. 4) Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari masa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	ICTSO dan Pentadbir ICT

KENYATAAN	TINDAKAN
K08/07/03 – Sistem Log	
1) 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). 2) Pentadbir Sistem hendaklah melaksanakan perkara-perkara berikut: (i) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (ii) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (iii) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO, Pengurus ICT dan CDO.	Pentadbir ICT
K08/07/04 – Pemantauan Log	
1) Ianya bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut: (i) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (ii) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu di wujud dan hasilnya perlu dipantau secara berkala; (iii) Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (iv) Aktiviti pentadbiran dan operator/pengendali sistem perlu direkodkan; (v) Kesalahan, kesilapan dan / atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya; dan (vi) Penyelarasan masa bagi domain keselamatan perlu menggunakan sumber masa yang sama (*time synchronization*).	ICTSO dan Pentadbir ICT

KAWALAN
09

KESELAMATAN KOMUNIKASI

COMMUNICATION SECURITY

KAWALAN 09 – KESELAMATAN KOMUNIKASI (*COMMUNICATION SECURITY*)

OBJEKTIF:

1) Mengawal aplikasi dan melindungi maklumat dalam rangkaian dan infrastruktur sokongan supaya sebarang risiko seperti penyalahgunaan maklumat serta pindaan yang tidak sah dapat dihalang.

2) Memastikan keselamatan pertukaran maklumat dan perisian antara APAD dan pihak ketiga terjamin disamping keselamatan dan kawalan penyebaran maklumat melalui media sosial.

KENYATAAN	TINDAKAN
K09/01 – PENGURUSAN KESELAMATAN RANGKAIAN	
K09/01/01 – Kawalan Infrastruktur Rangkaian	
1) Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. 2) Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: (i) Semua tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (ii) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; (iii) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (iv) *Firewall* hendaklah dipasang serta di konfigurasi dan diselia oleh Pentadbir Sistem; (v) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan APAD; (vi) Semua perisian *sniffer* atau *network analyser, proxy* dan sebarang perisian penggodam adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;	ICTSO dan Pentadbir Rangkaian

KENYATAAN	TINDAKAN
(vii) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat APAD; (viii) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (ix) Sebarang penyambungan dan penggunaan rangkaian yang bukan di bawah kawalan APAD adalah tidak dibenarkan kecuali dengan kebenaran khas ICTSO; (x) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan dan mematuhi pekeliling yang berkenaan; (xi) Aktiviti melayari laman sesawang yang dilarang seperti pronografi, perjudian atau keganasan perlu disekat menggunakan peralatan keselamatan; dan (xii) Pengurusan keselamatan perkhidmatan APAD tidak membenarkan penggunaan perkhidmatan perkomputeran awan dan haruslah merujuk kepada Garis Panduan Pengkomputeran Awan (Cloud Computing).	
K09/02 – Pengurusan Pertukaran Maklumat	
K09/02/01 – Pengurusan Penghantaran dan Pertukaran Maklumat	
1) Bertujuan untuk memastikan keselamatan penghantaran dan penerimaan maklumat dan perisian dalam APAD dan mana-mana entiti luar terjamin. 2) Langkah-langkah yang perlu dipatuhi adalah seperti berikut : (i) Mengenal pasti jenis aset maklumat yang dibenarkan untuk dikongsi oleh APAD serta melakukan pemantauan dan pengawalan terhadap aset tersebut secara berterusan; (ii) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (iii) Perjanjian yang jelas perlu diwujudkan untuk pertukaran maklumat dan perisian di antara APAD dengan pihak ketiga yang digunakan terjamin sepanjang akses dibenarkan dan seterusnya memulangkan kembali semula aset maklumat sekiranya kontrak telah tamat atau ditamatkan; (iv) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari APAD; dan (v) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	ICTSO, Pemilik Projek, Pentadbir ICT dan Warga APAD

KENYATAAN	TINDAKAN
K09/02/02 – Pengurusan Mel Elektronik (E-mel)	
1) Penggunaan mel elektronik (e-mel) di APAD hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan internet yang terkandung dalam Tatacara Penggunaan E-Mel Dan Internet (Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"). 2) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Hanya warga APAD atau pengguna yang dibenarkan sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi Agensi; (ii) Menggunakan akaun atau alamat e-mel yang diperuntukkan oleh APAD bagi urusan rasmi SAHAJA dan tujuan peribadi adalah tidak dibenarkan; (iii) Mengenalpasti, mengesahkan identiti pengguna sebelum meneruskan transaksi dan mengelakkan daripada membuka e-mel dari penghantar yang tidak diketahui dan diragui; (iv) Pengguna bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing; (v) Memastikan tarikh dan masa sistem komputer adalah tepat; (vi) E-mel rasmi yang dihantar atau diterima hendaklah disimpan dan diarkibkan mengikut panduan yang digariskan; (vii) Mengehadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan e-mel *bombing*; (viii) Penghantaran lampiran dalam format atau extension "*.bat, *.exe dan *.com" tidak dibenarkan; (ix) Menggunakan kaedah enkripsi (*encryption*) bagi dokumen terperingkat yang dihantar secara elektronik; (x) Pengemaskinian e-mel hendaklah dibuat sekiranya *mailbox* pengguna tidak aktif selama satu (1) bulan kecuali menerima pemakluman rasmi bagi mengesahkan pengguna *mailbox* masih aktif; dan (xi) Unit Pengurusan Sumber Manusia, Bahagian Khidmat Pengurusan perlu memaklumkan sebarang status pengguna (bertukar agensi, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke APAD dan tamat kontrak) bagi tujuan pengemaskinian e-mel yang terlibat.	Pentadbir ICT dan Warga APAD

KENYATAAN	TINDAKAN
K09/03 – Perkhidmatan Dalam Talian (Online Services)	
K09/03/01 – Perkhidmatan Dalam Talian	
1) Bagi menggalakkan pertumbuhan perkhidmatan dalam talian serta sebagai menyokong hasrat kerajaan mengoptimumkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. 2) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Memastikan maklumat yang terlibat dalam transaksi perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (ii) 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 (iii) Memastikan kerahsiaan dan integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi, misalnya dengan penggunaan Sijil Digital Pelayan yang sah atau PKI untuk mencegah sebarang pindaan yang tidak diperakukan.	CDO, ICTSO, Pengurus ICT, Pemilik Projek, Pentadbir ICT, Warga APAD dan Pihak Ketiga
K09/03/02 – Maklumat Umum	
1) Perkara perkara yang perlu dipatuhi dalam memastikan keselamatan siber adalah seperti berikut: (i) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (ii) Mengesahkan dan mendapat kelulusan untuk segala maklumat yang hendak dipaparkan sebelum dimuat naik ke laman web; dan (iii) Menguji sistem yang boleh diakses oleh orang awam terlebih dahulu untuk memastikan segala maklumat yang dipaparkan adalah seperti yang telah disah dan diluluskan sebelum dimuat naik ke laman web.	CDO, ICTSO, Pemilik Projek, Pentadbir ICT, Pengguna dan Pelanggan
K09/03/03 – Media Sosial	
1) Memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi dan disebarkan melalui media social adalah dipatuhi. 2) Warga APAD boleh merujuk kepada dokumen **Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam** yang dikeluarkan oleh pihak Jabatan Digital Negara (JDN).	Warga APAD dan Pihak Ketiga

KENYATAAN	TINDAKAN
3) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara; (ii) Tidak melibatkan penyebaran maklumat dan dokumen terperingkat; (iii) Tidak memaparkan kenyataan yang boleh menjejaskan imej kerajaan; (iv) Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; dan (v) Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan.	

KAWALAN
10

PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

KAWALAN 10 – PEMEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM (*SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE*)

OBJEKTIF:

1) Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

2) Memastikan pembangunan sistem alikasi secara in-houce dan outsource perlu diselia dan dipantau untuk memastikan ia mengikut jadual dan prosedur yang telah ditetapkan.

3) Memastikan supaya perubahan kawalan fail sistem dikawal dan dikendalikan dengan baik dan selamat disamping kawalan teknikal keterdedahan (vulnerability) adalah berkesan, sistematik dan berkala.

KENYATAAN	TINDAKAN
K10/01 – Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
K10/01/01 – Keperluan Keselamatan Sistem Aplikasi	
1) Maklumat mengenai Pengurusan Keselamatan Projek adalah mengikut Garis Panduan Pengurusan Projek ICT (PPrISA) yang dikeluarkan oleh Jabatan Digital Negara (JDN). 2) Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (i) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (ii) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat;	CDO, ICTSO, Pengurus ICT dan Pemilik Projek

KENYATAAN	TINDAKAN
(iii) Memastikan aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (iv) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan dan dalam tempoh penyelenggaraan.	
K10/01/02 – Pengesahan Data Input dan Data Output	
1) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan (ii) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	ICTSO, Pentadbir Sistem, Pemilik Sistem dan Pengguna
K10/01/03 – Kawalan Fail Sistem	
1) Fail sistem perlu dikawal dan dikendalikan dengan baik dan selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (i) Memastikan perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi dikawal, diuji, direkod dan disahkan sebelum diguna pakai; (ii) Proses pengemaskini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (iii) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; (iv) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (v) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; (vi) Memastikan data ujian perlu dipilih dan penggunaanya dikawal serta dilindungi; dan (vii) Menghalang sebarang peluang untuk membocorkan maklumat.	Pemilik Sistem dan Pentadbir Sistem ICT
K10/02 – Keselamatan Dalam Proses Pembangunan dan Sokongan	
K10/02/01 – Peraturan Keselamatan Dalam Pembangunan Sistem	
1) Peraturan bagi pembangunan sistem aplikasi hendaklah disediakan dan digunakan untuk pembangunna dalam organisasi.	ICTSO, Pemilik Projek dan Pentadbir ICT

KENYATAAN	TINDAKAN
2) Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: (i) Memastikan pembangunan sistem menggunakan teknik secure coding; (ii) Memastikan keselamatan pada persekitaran pembangunan sistem aplikasi dan pangkalan data; (iii) Mengetahui keperluan pengetahuan ke atas keselamatan sistem aplikasi dan keselamatan kawalan versi; dan (iv) Memastikan semua sistem baru dan penambahbaikan sistem menjalani ujian penerimaan sistem bagi memastikan garis panduan keselamatan dipenuhi serta lulus *User Acceptance Test* (UAT) dan *Final AcceptanceTest* (FAT) sebelum sistem diguna pakai.	
K10/02/02 – Pembangunan Secara Outsource	
1) Pembangunan perisian aplikasi secara outsource perlu mematuhi perkara-perkara berikut: (i) Memastikan setiap projek perlu dipantau oleh Pengurus ICT; (ii) Memastikan kod sumber, data/maklumat, prosedur dan dokumen yang dibangunkan oleh Pihak Ketiga adalah hak milik APAD dan dimasukkan klausa di dalam kontrak pembekalan; (iii) Kod sumber yang diserahkan kepada APAD mesti bebas daripada sebarang ralat dan kerentanan; (iv) Mengutamakan kepakaran teknologi tempatan; (v) Pembangunan aplikasi hendaklah dijalankan dalam persekitaran APAD mengikut situasi; (vi) Perlu penggunaan *data masking/ dummy data* semasa pembangunan dan penggujian; (vii) Data ujian hendaklah dilupuskan secara kekal (*secured delete*) selepas projek disiapkan/ tamat kontrak; (viii) Aktiviti sandaran penuh (*full backup*) ke atas keseluruhan sistem hendaklah berjaya dilakukan sebelum projek tamat; dan (ix) Setiap sistem, aplikasi dan perisian perlu mematuhi garis panduan keselamatan dan lulus *User Acceptance Test* (UAT) dan *Final AcceptanceTest* (FAT).	ICTSO, Pengurus ICT, Pentadbir ICT, Pemilik Sistem dan Pembekal
K10/02/03 – Pembangunan Aplikasi Mudah Alih	
1) Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk mesti menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang mengurangkan risiko ancaman keselamatan.	ICTSO, Pengurus ICT, Pentadbir ICT, Pemilik Sistem, Pembekal dan Pihak Ketiga

KENYATAAN	TINDAKAN
K10/03 – Kawalan Perubahan Fail Sistem, Teknikal dan Perisian	
K10/03/01 – Prosedur Kawalan Perubahan Terhadap Fail Sistem dan Perisian	
1) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Perubahan atau pengubahsuaian ke atas kitaran hayat pembangunan sistem, sistem pengoperasian dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai mengikut prosedur yang telah ditetapkan; (ii) Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan; (iii) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi; (iv) Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; (v) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (vi) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; (vii) Prinsip kejuruteraan keselamatan sistem hendaklah dibangunkan, didokumenkan, dikaji dan diguna pakai ke atas semua pelaksanaan sistem maklumat; (viii) Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem; dan (ix) Menghalang sebarang peluang untuk membocorkan maklumat.	Pengurus ICT, ICTSO, Pemilik Sistem dan Pentadbir Sistem ICT
K10/03/02 – Kawalan Teknikal Keterdedahan (*Vulnerability*)	
1) Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. 2) Perkara yang perlu dipatuhi adalah seperti berikut: (i) Memperoleh maklumat teknikal keterdedahan yang tepat dan terkini ke atas sistem maklumat yang digunakan; (ii) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; (iii) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan; dan (iv) Melaksanakan aktiviti *Security Posture Assessment* (SPA) perlu dilaksanakan sekurang-kurangnya sekali setahun.	ICTSO, Pengurus ICT, Pemilik Projek, Pentadbir ICT dan Pembekal

KAWALAN
11

HUBUNGAN PEMBEKAL

SUPPLIER RELATIONSHIP

KAWALAN 11 – HUBUNGAN PEMBEKAL (*SUPPLIER RELATIONSHIP*)

OBJEKTIF:

1) Memastikan keselamatan aset ICT APAD yang diberi kebenaran capaian dilindungi dari ancaman keselamatan.

2) Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan siber dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal.

KENYATAAN	TINDAKAN
K11/01 – Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	
K11/01/01 – Keselamatan Maklumat Berkaitan Hubungan Pembekal	
1) Seksyen ini menjelaskan keperluan untuk mendokumentasikan strategik mitigasi risiko keselamatan siber bila mana pembekal dibenarkan untuk mengakses ke aset APAD. 2) Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (i) Pembekal dan pengurusan pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas dan tertakluk kepada peraturan yang sedang berkuat kuasa; (ii) Mengenal pasti, mengawal dan memantau jenis aset maklumat yang dibenarkan untuk diakses oleh pembekal serta melakukan pemantauan terhadap aset tersebut secara berterusan; (iii) Mengadakan latihan kesedaran kepada semua pihak yang terlibat (APAD dan pembekal) untuk mendedahkan mereka dengan polisi, proses dan prosedur berkaitan keselamatan siber; (iv) Memastikan pemantauan berterusan dilakukan terhadap semua pembekal dengan melaksanakan pengukuran prestasi dan pematuhan terhadap garis panduan keselamatan siber; (v) Mewujudkan kontrak rasmi dan perjanjian yang jelas bersama pembekal bagi menjamin keselamatan siber APAD dan sepanjang akses yang dibenarkan serta seterusnya memulangkan kembali semula aset maklumat sekiranya kontrak mereka tamat atau ditamatkan dan segala urusan bersama pembekal dilaksanakan secara rasmi.	Unit Kewangan, Hasil dan Perolehan, Penasihat Undang-undang, JPICT, Pengurus ICT, ICTSO, Pemilik Projek, Pentadbir ICT dan Pembekal

KENYATAAN	TINDAKAN
K11/01/02 – Rangkaian Pembekal ICT	
1) Seksyen ini menjelaskan kandungan perjanjian bersama pembekal yang perlu diwujudkan bagi memastikan risiko keselamatan siber berkaitan rangkaian pembekal khidmat ICT dan produk diambil kira. 2) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (i) Mengenalpasti keperluan keselamatan siber khusus berkaitan dengan perolehan rangkaian pembekal perkhidmatan dan produk ICT sebagai tambahan kepada keperluan umum keselamatan siber berkaitan hubungan sub-pembekal; (ii) Memastikan rangkaian pembekal yang terlibat dalam menyediakan perkhidmatan dan produk ICT berkongsi hal berkaitan keselamatan siber (polisi, prosedur, proses) kepada setiap aras pembekal termasuk sub-pembekal atau sub-sub-pembekal; (iii) Melaksanakan proses pemantauan rangkaian pembekal perkhidmatan dan produk ICT dengan kaedah yang berkesan bagi menjamin keperluan keselamatan siber sentiasa dipatuhi; (iv) Mendapatkan jaminan bahawa komponen produk yang kritikal boleh berfungsi mengikut spesifikasi dan dikesan sumbernya dari rangkaian pembekal yang pelbagai; dan (v) Menguruskan rangkaian pembekal perkhidmatan dan produk ICT bagi menjamin keselamatan siber dan kesinambungan perkhidmatan kerana perubahan trend dan teknologi.	Unit Kewangan, Hasil dan Perolehan, Penasihat Undang-undang, JPICT, CDO, Pengurus ICT, ICTSO, Pemilik Projek dan Pembekal
K11/02 – Pengurusan Penyampaian Perkhidmatan Pembekal	
K11/02/01 – Perkhidmatan Penyampaian	
1) Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (i) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan di selenggara oleh pihak ketiga; (ii) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau dan disemak secara berkala; dan (iii) Mengambil kira pengurusan perubahan dasar tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Unit Kewangan, Hasil dan Perolehan, Penasihat Undang-undang, JPICT, CDO, Pengurus ICT, ICTSO, Pemilik Projek dan Pembekal

KENYATAAN	TINDAKAN
K11/02/02– Pemantauan dan Kajian Perkhidmatan Pembekal	
1) APAD sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal. 2) Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (i) Memantau tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan; dan (ii) Memastikan laporan perkhidmatan yang dihasilkan oleh pembekal dipantau dan status kemajuan dikemukakan kepada APAD.	Unit Kewangan, Hasil dan Perolehan, Penasihat Undang-undang, JPICT, CDO, Pengurus ICT, ICTSO, Pemilik Projek dan Pembekal
K11/02/03 – Pengurusan Perubahan Perkhidmatan Pembekal	
1) Semua perubahan perkhidmatan pembekal dilaksanakan secara teratur dan mengikut klausa kontrak yang ditetapkan. 2) Perkara-perkara yang perlu diambil kira adalah seperti berikut: (i) Perubahan dalam perjanjian dengan pembekal; (ii) Perubahan yang dilakukan oleh APAD bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan (iii) Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, peralatan baharu, perubahan lokasi, perubahan pembekal dan subkontraktor.	Unit Kewangan, Hasil dan Perolehan, Penasihat Undang-undang, JPICT, CDO, Pengurus ICT, ICTSO, Pemilik Projek dan Pembekal

KAWALAN
12

RISIKO & PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

ICT SECURITY INCIDENT MANAGEMENT

KAWALAN 12 – RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT (*ICT SECURITY INCIDENT MANAGEMENT*)

OBJEKTIF:

1) Memastikan insiden dikendalikan dengan konsisten, cepat tepat dan berkesan termasuk saluran komunikasi keselamatan dan security events bagi meminimumkan kesan insiden keselamatan ICT.

2) Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

KENYATAAN	TINDAKAN
K12/01 – Mekanisme Pelaporan Insiden Keselamatan ICT	
K12/01/01 – Mekanisme Pelaporan	
1) Pelaporan (i) Insiden keselamatan siber bermaksud musibah (adverse event) yang berlaku ke atas aset ICT sama ada perkakasan, perisian atau ke atas kakitangan atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan siber ICT sama ada yang ditetapkan secara tersurat atau tersirat. (ii) Semua maklumat adalah SULIT dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan sahaja. (iii) Insiden keselamatan siber seperti berikut hendaklah dilaporkan kepada ICTSO/Pasukan CSIRT agensi dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak –pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisma kawalan akses: i. hilang, dicuri atau didedahkan; ii. disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan	ICTSO, CSIRT APAD, Warga APAD dan Pihak Ketiga

KENYATAAN	TINDAKAN
e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini yang boleh menjejaskan keselamatan siber. 2) Pelaporan NACSA (i) ICTSO melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT sekiranya perlu; dan (ii) Pasukan CSIRTAPAD dengan persetujuan ICTSO akan menghubungi NACSA untuk melaporkan atau mendapatkan bantuan apabila wujud potensi insiden atau berlaku sebarang insiden keselamatan siber. 3) Tindakan Dalam Keadaan Berisiko Tinggi (i) Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. (ii) Tindakan perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak. 4) Pelaporan kepada CSIRT APAD (i) Pentadbir sistem yang terlibat mesti melaporkan sebarang insiden yang melibatkan keselamatan siber kepada CSIRT APAD. 5) Prosedur pelaporan insiden keselamatan ICT berdasarkan: (i) Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Pengendalian Insiden Keselamatan Siber Sektor Awam. (ii) Pekeliling dan Prosedur yang dikeluarkan oleh pihak NACSA.	
K12/02 – Pengurusan Maklumat Insiden Keselamatan Siber	
K12/02/01 – Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
1) Pengurusan pengendalian insiden keselamatan siber dilaksanakan oleh Pasukan CSIRT APAD yang diketui oleh ICTSO. 2) Pengendalian ini dilaksana berpandukan prosedur pengurusan pelaporan dan pengendalian insiden keselamatan siber yang berkuatkuasa. 3) Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang.	ICTSO, CSIRT APAD

KENYATAAN	TINDAKAN
4) Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada APAD. 5) Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. 6) Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut; (i) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti; (ii) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (iii) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (iv) Menyediakan tindakan pemulihan segera; (v) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu. **Carta lengkap** mengenai perjalanan **laporan insiden** seperti di **Lampiran 3**; dan (vi) Pengurusan insiden yang tidak melibatkan insiden keselamatan siber adalah berdasarkan prosedur pengendalian insiden yang ditetapkan oleh pihak APAD. 7) Langkah-langkah yang diambil dalam pengurusan insiden adalah seperti berikut: (i) Menerima laporan insiden daripada pengguna, pihak NACSA atau sumber lain; (ii) Mengenal pasti semua jenis insiden keselamatan ICT; (iii) Mematuhi Pelan Pemulihan Bencana (DRP) seperti yang telah digariskan dalam PKP; (iv) Sekiranya insiden tersebut memerlukan tindakan susulan undang-undang, laporan perlu dipanjangkan kepada agensi penguatkuasa undang-undang; (v) Sekiranya memerlukan bantuan daripada NACSA atau agensi lain, permohonan perlu dihantar ke pihak NACSA dan Menyimpan jejak audit dan memelihara bahan bukti dan rekod; (vi) Menyediakan tindakan pencegahan supaya insiden serupa tidak berulang; dan (vii) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

KAWALAN
13

KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

INFORMATION SECURITY OF BUSINESS CONTINUITY MANAGEMENT

KAWALAN 13 – KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (*INFORMATION SECURITY OF BUSINESS CONTINUITY MANAGEMENT*)

OBJEKTIF:

1) Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

KENYATAAN	TINDAKAN
K13/01 – Dasar Kesinambungan Perkhidmatan	
K13/01/01 – Pelan Kesinambungan Perkhidmatan	
1) Pelan Kesinambungan Perkhidmatan - PKP (*Business Continuity Plan - BCP*) ialah mekanisma bagi mengurus dan memastikan kepentingan stakeholder sistem penyampaian perkhidmatan dilindungi dan imej APAD terpelihara. 2) Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan APAD di samping menyediakan pelan tindakan bagi mewujudkan ketahan dan keupayaan bertindak yang berkesan. 3) Ketua Pengarah adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT APAD. 4) Pelan ini perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (i) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (ii) Senarai personal APAD dan pembekal perkhidmatan berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personal tidak dapat hadir untuk menangani insiden; (iii) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;	CDO, Pengurus ICT, ICTSO, Pasukan Pemulihan Bencana (DRT) APAD dan Pihak Ketiga

KENYATAAN	TINDAKAN
(iv) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (v) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. 5) Salinan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. 6) 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. 7) Ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. 8) APAD hendaklah memastikan salinan PKP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	
K13/01/02 – Pelan Pemulihan Bencana	
1) Pelan Pemulihan Bencana (DRP) merujuk kepada dokumen pelan yang menetapkan sumber, tindakan, tanggungjawab dan data yang diperlukan untuk mengurus proses pemulihan selepas gangguan terhadap perkhidmatan kritikal APAD. 2) Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. (i) Pelan ini mestilah diluluskan oleh JPICT APAD dan perkara-perkara berikut perlu diberi perhatian: (ii) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (iii) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan siber; (iv) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (v) Mendokumentasikan proses dan prosedur yang telah dipersetujui;	Pasukan PKP, Pasukan Tindak Balas (ERT), ICTSO, Pasukan Pemulihan Bencana (DRT) APAD dan Pihak Ketiga

KENYATAAN	TINDAKAN
(vi) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (vii) Membuat backup; (viii) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali atau mengikut keperluan; dan	
K13/01/03 – Lewahan (*Redundancy*)	
Semua sistem aplikasi dan peralatan yang kritikal hendaklah mempunyai kemudahan lewahan dan diuji (failover test) keberkesanannya mengikut keperluan dan kesesuaian semasa.	Pengurus ICT dan Pentadbir Sistem

KAWALAN
14

PEMATUHAN

COMPLIANCE

KAWALAN 14 – PEMATUHAN (COMPLIANCE)

OBJEKTIF:

1) Meningkatkan tahap keselamatan ICT bagi mengelakkan sebarang pelanggaran kepada DKICT APAD.

2) Memastikan keselamatan siber dilaksanakan mengikut polisi dan prosedur APAD.

KENYATAAN	TINDAKAN
K14/01 – Pematuhan dan Keperluan Perundangan	
K14/01/01 – Pematuhan Dasar	
1) Setiap pengguna APAD hendaklah membaca, memahami dan mematuhi PKS APAD dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. 2) Semua aset APAD termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. 3) Ketua Jabatan atau pegawai yang diturunkan kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. 4) Sebarang penggunaan aset APAD selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber APAD. 5) Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga APAD adalah seperti di Lampiran 4 tertakluk kepada kesesuaian APAD. 6) Perkara yang perlu dipatuhi adalah seperti berikut: (i) Semua perlembagaan, undang-undang, peraturan, perjanjian yang dimeterai dan lain-lain perkara yang relevan kepada keselamatan sistem maklumat dan organisasi hendaklah dikenal pasti, didokumenkan dan dikemas kini; (ii) Peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan perjanjian mengenai penggunaan material yang tertakluk kepada hak milik harta intelek; (iii) Rekod penting hendaklah dilindungi daripada hilang, rosak atau dipalsukan selaras dengan keperluan undang-undang, peraturan dan keperluan perjanjian APAD;	CDO, Pengurus ICT, ICTSO, Warga APAD dan Pengguna

KENYATAAN	TINDAKAN
(iv) Perlindungan ke atas data dan maklumat privasi hendaklah mematuhi perundangan, peraturan dan terma perjanjian jika perlu; dan (v) Penggunaan kriptografi perlu dikawal selia selaras dengan perjanjian, perundangan dan peraturan yang berkuat kuasa.	
K14/01/02 – Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal Keselamatan	
1) ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. 2) Sistem ICT maklumat perlu melalui penilaian pemeriksaan secara berkala bagi memastikan standard pelaksanaan keselamatan ICT sentiasa dipatuhi. 3) Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment* (SPA) mestilah dijalankan oleh pihak yang kompeten dan dibenarkan oleh APAD.	ICTSO
K14/01/03 – Pematuhan Keperluan Audit	
1) Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem ICT. 2) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui ICTSO bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. 3) Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO dan Warga APAD
K14/01/04 – Pelanggaran Perundangan	
1) Mengenal pasti pelanggaran PKS APAD boleh dikenakan tindakan tatatertib. 2) Pelanggaran dasar ini boleh dikenakan di bawah **Akta Rahsia Rasmi 1972 [Akta 88], Perintah-perintah Am Bab "D" – Peraturan-peraturan Pegawai Awam (Kelakuan dan Tatatertib) dan Arahan Keselamatan Kerajaan.**	Warga APAD
K14/01/05– Hak Harta Intelek (*Intellectual Property Rights* – IPR)	
1) Prosedur-prosedur yang sesuai akan dilaksanakan untuk memastikan keselarasan dengan perundangan, peraturan dan juga keperluan kontrak yang berkaitan dengan *Intellectual Property Rights* (IPR) dan juga pelesenan perisian.	Warga APAD

KENYATAAN	TINDAKAN
2) APAD akan mengiktiraf dan menghormati hak-hak intelek yang berkaitan dengan sistem maklumat. 3) Perkara-perkara berikut perlu dipatuhi: (i) Memastikan pematuhan terhadap hak cipta yang berkaitan dengan perisian propretari dan reka bentuk untuk kegunaan APAD; (ii) Memastikan pematuhan terhadap pelesenan menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperolehi untuk kegunaan APAD; dan (iii) Memastikan pengguna tidak dibenarkan menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan.	
K14/02 – Kajian Keselamatan Maklumat	
K14/02/01 – Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat	
1) Dalam pelaksanaan keselamatan siber APAD, kesemua prosedur, polisi dan proses keselamatan siber disemak apabila terdapat perubahan ketara berlaku dalam pelaksanaannya. 2) ICTSO memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.	JPICT dan ICTSO
K14/02/02 – Pematuhan Kajian Teknikal	
Aset ICT sentiasa dikaji supaya selaras dengan pematuhan polisi dan piawaian keselamatan siber APAD (seperti *Security Posture Assessment* – SPA)	ICTSO, Pengurus ICT, Pemilik Projek dan Pentadbir ICT

GLOSARI / TERMA RUJUKAN

PKS V1.0

GLOSARI / TERMA RUJUKAN

ISTILAH	PENERANGAN
APAD	Agensi Pengangkutan Awam Darat Organisasi APAD merangkumi bahagian-bahagian seperti berikut: (i) Pejabat Ketua Pengarah; (ii) Pejabat Ketua Pengarah Pembangunan; (iii) Pejabat Ketua Pengarah Operasi; (iv) Bahagian Khidmat Pengurusan (BKP); (v) Unit Undang-undang; (vi) Unit Komunikasi Korporat; (vii) Unit Integriti; (viii) Bahagian Aplikasi Teknologi; (ix) Bahagian Perancangan Polisi Mod Jalan; (x) Bahagian Perancangan Rel; (xi) Bahagian Penguatkuasaan Rel; (xii) Bahagian Pengangkutan Awam dan Perdagangan (BPAD); (xiii) Bahagian Bas Ekspres dan Terminal; dan (xiv) Bahagian Pelesenan Komersil.
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM 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	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
BCP	*Business Continuity Plan* Pelan tindakan bagi memastikan Kesinambungan Perkhidmatan.

ISTILAH	PENERANGAN
Bilik Khas	Bilik yang selamat dan terkawal.
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.
CDO/CIO	*Chief Digital Officer/ Chief Information Officer* Ketua Pegawai Digital/ Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi bagi mewujudkan budaya kerja yang dipacu oleh digital.
CGSO	*Malaysia Office of the Chief Government Security Officer* Ketua Pegawai Keselamatan Kerajaan Malaysia
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.
CNII	*Critical National Information Infrastruktur* Infrastruktur Maklumat Kritikal Negara dimana sistem yang merangkumi aset maklumat (elektronik), rangkaian, fungsi, proses, kemudahan dan perkhidmatan dalam persekitaran teknologi maklumat dan komunikasi.
CSIRT APAD	*Cyber Security Incident Response Team* Jawatankuasa yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
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 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 sedang diperbaharui, diproses, dihapus, diakses atau dibaca oleh sistem. Jenis data ini tidak disimpan secara pasif tetapi bergerak aktif melalui infrastruktur IT.

ISTILAH	PENERANGAN
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 Planning* Pelan tindakan untuk mencegah dan memulih.
Dummy Data	*Dummy* data ialah data yang tidak bermakna yang digunakan untuk tujuan pengujian dan latihan.
Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk peralatan 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.
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
ICTSO	*ICT Security Officer* 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.

ISTILAH	PENERANGAN
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.
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 Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman keselamatan ICT yang boleh menjejaskan kelancaran operasi dan sistem ICT APAD.
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (piawaian format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out computer* Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.
MODEM	*MOdulator DEModulator* Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
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.

ISTILAH	PENERANGAN
NACSA	*National Cyber Security Agency* Agensi Keselamatan Siber Negara
NC4	*National Cyber Coordination and Command Centre* Pusat Kawalan dan Penyelarasan Siber Negara
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
PDSA	Pusat Data Sektor Awam
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	Menyelaras dan memastikan urusan keselamatan perlindungan di APAD terjamin, teratur, cekap dan berkesan mengikut tatacara dan peraturan yang ditetapkan sepanjang masa.
Pekerja Sementara	Pegawai Khidmat Sambilan (PKS)/Pegawai Sambilan Harian (PSH)
Pembangun Sistem	Individu atau kumpulan teknikal atau pihak luaran yang bertanggungjawab dalam membangunkan sistem aplikasi berdasarkan spesifikasi keperluan sistem yang ditetapkan oleh pemohon/pemilik proses.
Pembekal	Pembekal barangan atau penyedia perkhidmatan.
Pemilik	Pegawai yang didaftarkan sebagai pemilik aset dan dipertanggungjawabkan ke atas aset tersebut.
Pemilik Projek	Individu yang bertanggungjawab terhadap hampir keseluruhan proses kerja projek tersebut. Pemilik projek memainkan peranan utama menentukan keperluan, spesifikasi dan ciri-ciri serahan (produk atau perkhidmatan) yang akan dihasilkan oleh projek tersebut.
Pemilik Proses	Individu yang bertanggungjawab untuk menentukan keperluan bisnes dan mengesahkan sebarang perubahan yang diperlukan berkaitan dengan bisnes proses.
Pengguna	Pengguna terdiri daripada warga APAD dan pihak ketiga yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT APAD.
Pengurus ICT	Pegawai yang mengetuai organisasi ICT di Agensi/ Bahagian/ Unit berkaitan ICT.
Pengurus Projek	Individu yang bertanggungjawab untuk merancang dan menguruskan projek dengan baik supaya projek dapat disiapkan mengikut kos, tempoh masa dan kualiti yang telah ditetapkan.
Pentadbir Sistem	Individu atau kumpulan teknikal yang bertanggungjawab mentadbir, mengurus dan menyenggara merangkumi fungsi dan peranan seperti berikut:

ISTILAH	PENERANGAN
	(i) Pentadbir Rangkaian dan Keselamatan; (ii) Pentadbir Pusat Data; (iii) Pegawai Aset; dan (iv) Pentadbir Sistem Aplikasi;
Peralatan Sokongan ICT	Peralatan yang menyokong penggunaan peralatan ICT bagi memastikan kelancaran ICT contohnya projektor, layar, kabel, speaker dan mikrofon.
Perisian	Program atau atur cara komputer yang dapat digunakan dengan sistem komputer tertentu.
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 Kementerian.
Pihak Ketiga	Terdiri daripada Pembekal perkhidmatan/Pakar runding/Agensi luar atau mana-mana pihak yang mempunyai urusan dengan perkhidmatan digital APAD atas urusan rasmi
PII	*Personally Identifiable Information* Maklumat Pengenalan Peribadi
PKS	Polisi Keselamatan Siber
PKP	Pengurusan Kesinambungan Perkhidmatan
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perrkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Pusat Data	Pengurusan pusat data APAD dengan menggunakan kemudahan yang disediakan oleh Jabatan Digital Negara. Pusat data yang digunakan adalah PDSA Cyberjaya, PDSA Putrajaya, PDSA Enstek dan PDSA Kulim.
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 ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer.
Sistem	Kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple*

ISTILAH	PENERANGAN
	Access/Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Switch	Alat yang boleh menapis (*filter*) dan memajukan (*forward*) isyarat paket data antara segmen rangkaian LAN.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
WAN	*Wide Area Network* Rangkaian Kawasan Luas yang menghubungkan komputer yang berada pada lokasi yang berbeza seperti negeri, negara dan benua.
Warga APAD	Pegawai/Kakitangan yang berkhidmat di APAD.
Wireless	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.

SENARAI PERUNDANGAN & PERATURAN

PKS V1.0

SENARAI PERUNDANGAN DAN PERATURAN

SENARAI PERUNDANGAN DAN PERATURAN	
1.	PERINTAH-PERINTAH AM;
2.	AKTA 56 – AKTA KETERANGAN 1950;
3.	AKTA 88 – AKTA RAHSIA RASMI 1972;
4.	AKTA 298 – KAWASAN LARANGAN TEMPAT LARANGAN 1959;
5.	AKTA 332 – AKTA HAK CIPTA (PINDAAN) TAHUN 1997;
6.	AKTA 562 – AKTA TANDATANGAN DIGITAL 1997;
7.	AKTA 563 – AKTA JENAYAH KOMPUTER 1997;
8.	AKTA 588 – AKTA KOMUNIKASI DAN MULTIMEDIA 1998;
9.	AKTA 606 – AKTA CAKERA OPTIK 2000;
10.	AKTA 629 – AKTA ARKIB NEGARA 2003;
11.	AKTA 658 – AKTA PERDAGANGAN ELEKTRONIK 2006;
12.	AKTA 680 – AKTA AKTIVITI KERAJAAN ELEKTRONIK 2007 (ARAHAN TEKNOLOGI MAKLUMAT 2007);
13.	AKTA 709 – AKTA PELINDUNGAN DATA PERIBADI 2010;
14.	AKTA 854 – AKTA KESELAMATAN SIBER 2024;
15.	ARAHAN KESELAMATAN (SEMAKAN DAN PINDAAN 2017);
16.	ARAHAN NO. 20 (SEMAKAN SEMULA) – DASAR DAN MEKANISMA PENGURUSAN BENCANA NEGARA;
17.	ARAHAN NO. 24 – DASAR DAN MEKANISMA PENGURUSAN KRISIS SIBER NEGARA;
18.	DASAR PENGURUSAN REKOD DAN ARKIB ELEKTRONIK;
19.	ETIKA PENGGUNAAN E-MEL DAN INTRANET APAD;
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. POLISI KESELAMATAN SIBER JABATAN DIGITAL NEGARA (JDN);
28. PROSEDUR PENGURUSAN PELAPORAN DAN PENGENDALIAN INSIDEN KESELAMATAN ICT APAD;
29. RANGKA KERJA KESELAMATAN SIBER SEKTOR AWAM (RAKKSSA) VERSI 1.0;
30. DIRECTIVE NO. 26, THE NATIONAL CYBER COORDINATION AND COMMAND CENTRE (NC4) IS ALSO DESIGNATED AS MALAYSIA'S NATIONAL COMPUTER EMERGENCY RESPONSE TEAM (CERT);
31. PERATURAN-PERATURAN PEGAWAI AWAM (PERLANTIKAN, KENAIKAN PANGKAT PENAMATAN PERKHIDMATAN) 2005
32. PERATURAN-PERATURAN PEGAWAI AWAM (KELAKUAN DAN TATATERTIB) 1993
33. PANDUAN PENGURUSAN PEJABAT (PEKELILING PERKHIDMATAN BIL. 5 TAHUN 2007)
34. PEKELILING KEMAJUAN PENTADBIRAN AWAM (PKPA)
35. PEKELILING PERKHIDMATAN SUMBER MANUSIA (MyPPSM)
36. PEKELILING PERKHIDMATAN DAN SURAT PEKELILING PERKHIDMATAN
37. PEKELILING AM DAN SURAT PEKELILING AM
38. PEKELILING PERBENDAHARAAN (PPP)
39. ARAHAN PERBENDAHARAAN
40. AKTA PROSEDUR KEWANGAN 1957

PEKELILING AM

1. PEKELILING AM BILANGAN 6 TAHUN 1999, PELAKSANAAN PERKONGSIAN PINTAR ANTARA AGENSI-AGENSI KERAJAAN DALAM BIDANG TEKNOLOGI MAKLUMAT
2. PEKELILING AM BIL. 3 TAHUN 2000 RANGKA DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI KERAJAAN (ICT)
3. PEKELILING AM BIL.4 TAHUN 2022 PENGURUSAN DAN PENGENDALIAN INSIDEN KESELAMATAN SIBER SEKTOR AWAM
4. PEKELILING AM BIL. 2 TAHUN 2002, PENGGUNAAN DAN PEMAKAIAN DATA DICTIONARY SEKTOR AWAM (DDSA) SEBAGAI STANDARD DI AGENSI-AGENSI KERAJAAN.
5. PEKELILING AM BILANGAN 2 TAHUN 2006, PENGUKUHAN TADBIR URUS JAWATANKUASA IT DAN INTERNET KERAJAAN
6. PEKELILING AM BIL. 1 TAHUN 2015, PELAKSANAAN DATA TERBUKA SEKTOR AWAM

7.	MALAYSIAN PUBLIC SECTOR MANAGEMENT OF INFORMATION & COMMUNICATIONS TECHNOLOGY SECURITY HANDBOOK (MyMIS)
	SURAT PEKELILING AM
1.	SURAT PEKELILING AM BIL. 4 TAHUN 2006, PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) SEKTOR AWAM
2.	SURAT PEKELILING AM BIL. 3 TAHUN 2009, GARIS PANDUAN PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM
3.	SURAT PEKELILING AM BILANGAN 3 TAHUN 2015, GARIS PANDUAN PERMOHONAN KELULUSAN TEKNIKAL DAN PEMANTAUAN PROJEK TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) AGENSI SEKTOR AWAM
4.	SURAT PEKELILING AM BILANGAN 3 TAHUN 2024 – GARIS PANDUAN PENGURUSAN RISIKO KESELAMATAN MAKLUMAT SEKTOR AWAM BERTARIKH 21 MAC 2024
	PEKELILING KEMAJUAN PENTADBIRAN AWAM (PKPA)
1.	PEKELILING KEMAJUAN PENTADBIRAN AWAM BIL. 1 TAHUN 2003, GARIS PANDUAN MENGENAI TATACARA PENGGUNAAN INTERNET DAN MEL ELEKTRONIK DI AGENSI-AGENSI KERAJAAN
2.	PEKELILING KEMAJUAN PENTADBIRAN AWAM BIL. 2 TAHUN 2015, PENGURUSAN LAMAN WEB AGENSI SEKTOR AWAM
3.	PEKELILING TRANSFORMASI PENTADBIRAN AWAM, BIL. 3 TAHUN 2017 PENGURUSAN PERKHIDMATAN KOMUNIKASI BERSEPADU KERAJAAN (*GOVERNMENT UNIFIED COMMUNICATION*)
4.	PEKELILING TRANSFORMASI PENTADBIRAN AWAM BIL. 4 TAHUN 2017, PELAKSANAAN KUMPULAN WANG AMANAH PEMBANGUNAN PROJEK ICT SEKTOR AWAM (KWAICT)
5.	PEKELILING TRANSFORMASI PENTADBIRAN AWAM BIL. 3 TAHUN 2018, PANDUAN PENGURUSAN PROJEK ICT SEKTOR AWAM (PPRISA)
	SURAT ARAHAN KETUA PENGARAH PERKHIDMATAN AWAM / KETUA PENGARAH MAMPU
1.	LANGKAH-LANGKAH MENGENAI PENGGUNAAN MEL ELEKTRONIK DI AGENSI-AGENSI KERAJAAN (JUN 2007)
2.	LANGKAH-LANGKAH PEMANTAPAN PELAKSANAAN SISTEM MEL ELEKTRONIK DI AGENSI-AGENSI KERAJAAN (NOVEMBER 2007)
3.	GARIS PANDUAN PELAKSANAAN BLOG BAGI AGENSI SEKTOR AWAM (JULAI 2009)
4.	PANDUAN PENYEDIAAN BERITA ONLINE DAN PENYIARAN BERITA ONLINE DI LAMAN WEBPORTAL AGENSI-AGENSI KERAJAAN (SEPTEMBER 2009)

5.	PENGGUNAAN MEDIA JARINGAN SOSIAL DI SEKTOR AWAM (NOVEMBER 2009)
6.	GARIS PANDUAN PENGGUNAAN ICT KE ARAH ICT HIJAU DALAM PERKHIDMATAN AWAM (2010)
7.	GARIS PANDUAN TRANSISI PROTOKOL INTERNET VERSI 6 (IPV6) SEKTOR AWAM (JANUARI 2010)
8.	PEMANTAPAN PENGGUNAAN DAN PENGURUSAN E-MEL DI AGENSI-AGENSI KERAJAAN (2010)
9.	AMALAN TERBAIK PENGGUNAAN MEDIA JARINGAN SOSIAL (TARIKH 8 APRIL 2011)

LAMPIRAN

LAMPIRAN

LAMPIRAN 1

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER, AGENSI PEGANGKUTAN AWAM DARAT (APAD)

KEMENTERIAN PENGANGKUTAN MALAYSIA

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian/Unit : .....

Organisasi (selain warga APAD) : .....

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

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya sedia maklum mengenai kewujudan Polisi Keselamatan Siber (PKS) APAD;
2. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam PKS APAD dan
3. 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

Agensi Pengangkutan Awam Darat

Kementerian Pengangkutan Malaysia

Tarikh : .....

Nota : Semua warga APAD perlu membaca PKS APAD secara keseluruhan sebelum menandatangani Surat Akuan Pematuhan Polisi ini. PKS APAD boleh di capai di Portal APAD pada pautan Our Services > Guidelines > ICT Security Policy

LAMPIRAN 2

BORANG NDA

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 atau 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 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 selesai.

Tandatangan : .....
Nama (huruf besar) : .....
No.Kad Pengenalan : .....
Jawatan : .....
Syarikat : .....
Tarikh : .....

Disaksikan oleh : .....
(Tandatangan)

Nama (huruf besar) : .....
No.Kad Pengenalan : .....
Jawatan : .....
Jabatan / Organisasi : .....
Tarikh : .....
Cop Jabatan / Organisasi : .....

LAMPIRAN 3

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 [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, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi 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 daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila tamat projek Kerajaan.

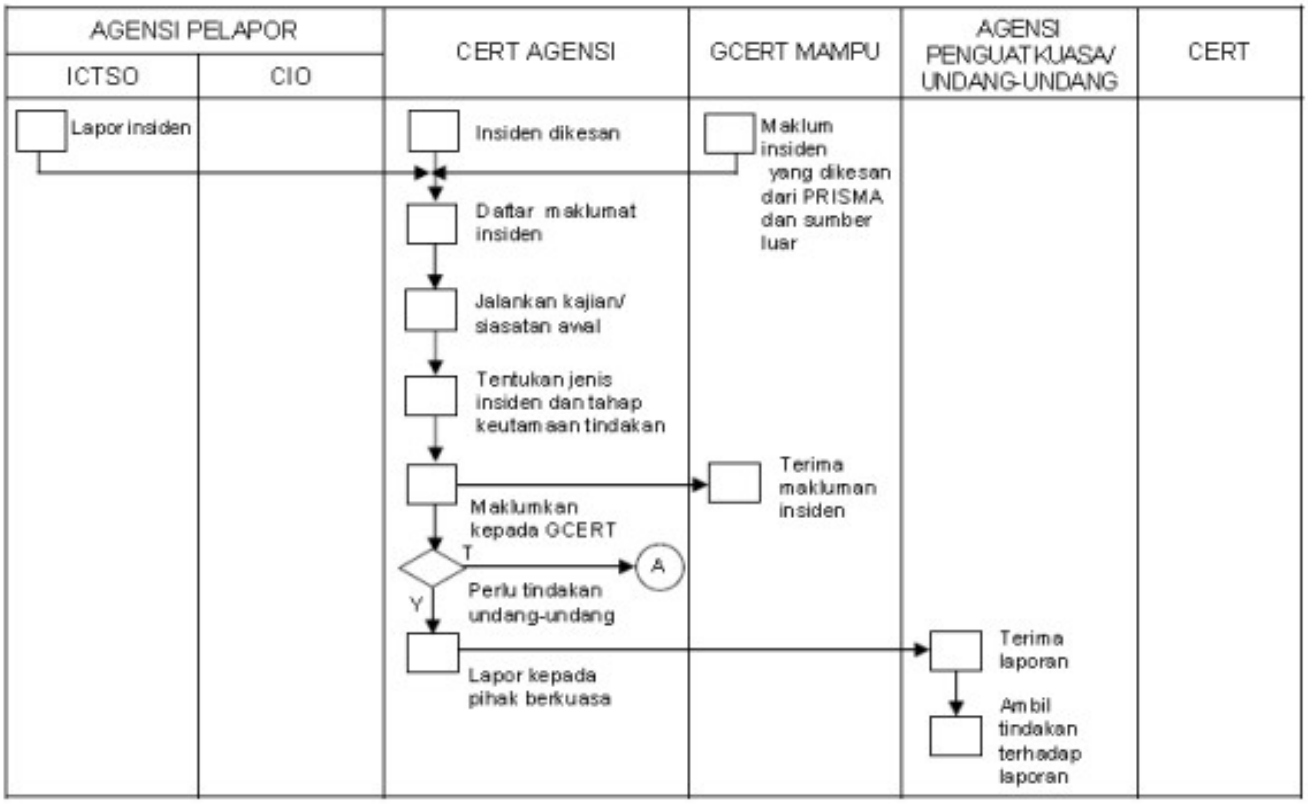
Tandatangan : .....
Nama (huruf besar) : .....
No.Kad Pengenalan : .....
Jawatan : .....
Syarikat : .....
Tarikh : .....

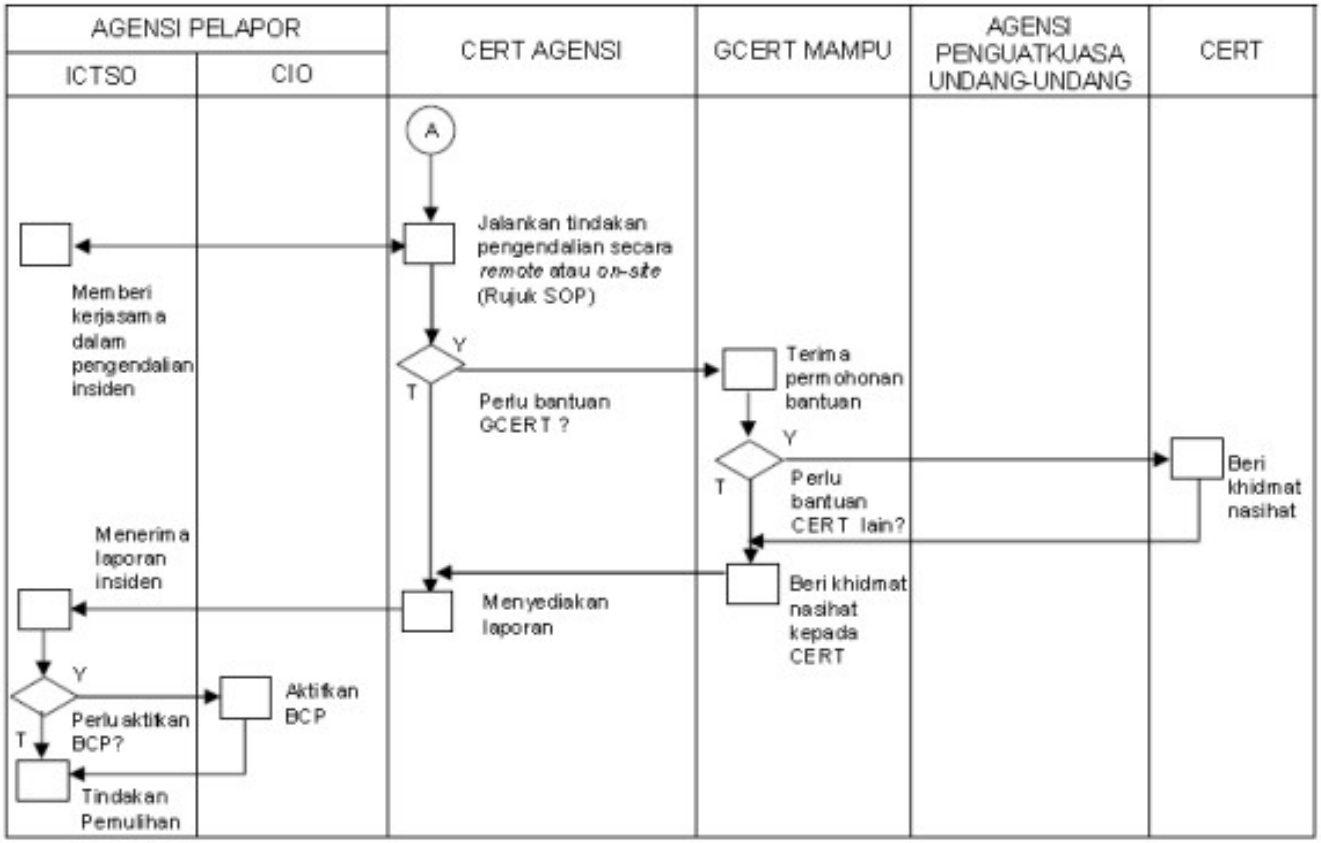
Disaksikan oleh : .....
(Tandatangan)

Nama (huruf besar) : .....
No.Kad Pengenalan : .....
Jawatan : .....
Jabatan / Organisasi : .....
Tarikh : .....
Cop Jabatan / Organisasi : .....

LAMPIRAN 4

RAJAH 1 : CARTA ALIR PROSES KERJA PELAPORAN INSIDEN KESELAMATAN SIBER




AGENSI PELAPOR
ICTSO
CIO
CERT AGENSI
GCERT MAMPU
AGENSI PENGUATKUASA UNDANG-UNDANG
CERT
A
Jalankan tindakan pengendalian secara *remote* atau *on-site* (Rujuk SOP)
Memberi kerjasama dalam pengendalian insiden
Y
T
Perlu bantuan GCERT ?
Terima permohonan bantuan
Y
T
Perlu bantuan CERT lain?
Beri khidmat nasihat
Menerima laporan insiden
Menyediakan laporan
Beri khidmat nasihat kepada CERT
Y
T
Perlu aktifkan BCP?
Aktifkan BCP
Tindakan Pemulihan

LAMPIRAN 5

BORANG PERMOHONAN PENGURUSAN EMEL (INDIVIDU)

AGENSI PENGANGKUTAN AWAM DARAT (APAD)

KEMENTERIAN PENGANGKUTAN MALAYSIA

BORANG PENGURUSAN EMEL (INDIVIDU)

Untuk Pemohon

A) Maklumat Pemohon: Tarikh: _____

Nama/Gelaran : _____

Alamat Penuh : _____

No Kad Pengenalan : _____ No Tel/HP : _____

Skim & Gred : _____ Jawatan : _____

Bahagian : _____ Cawangan/Unit : _____

B) Sila tandakan / ruangan dibawah:

	a. Permohonan Baru
	b. Pertukaran Dalaman
	c. Hapus (Nyatakan Sebab:.....)
	d. Reset Password (Nyatakan Sebab:.....)
	e. Kemaskini

Sila isikan ruangan di bawah jika memilih item b atau d di atas:

e-mel lama:	Lokasi Pejabat lama:

Pengesahan Ketua Jabatan / Pegawai Tadbir Bahagian:

T/Tangan : _____

Tarikh : _____ Nama dan Cop Jawatan:

UNTUK KEGUNAAN UPM

Tarikh Terima : Tarikh Selesai :

ID Baru:	e-mel Baru:
ID Lama:	e-mel Lama:
Lokasi Pejabat Lama:	Lokasi Pejabat Baru:

SALINAN KEPADA PENGGUNA

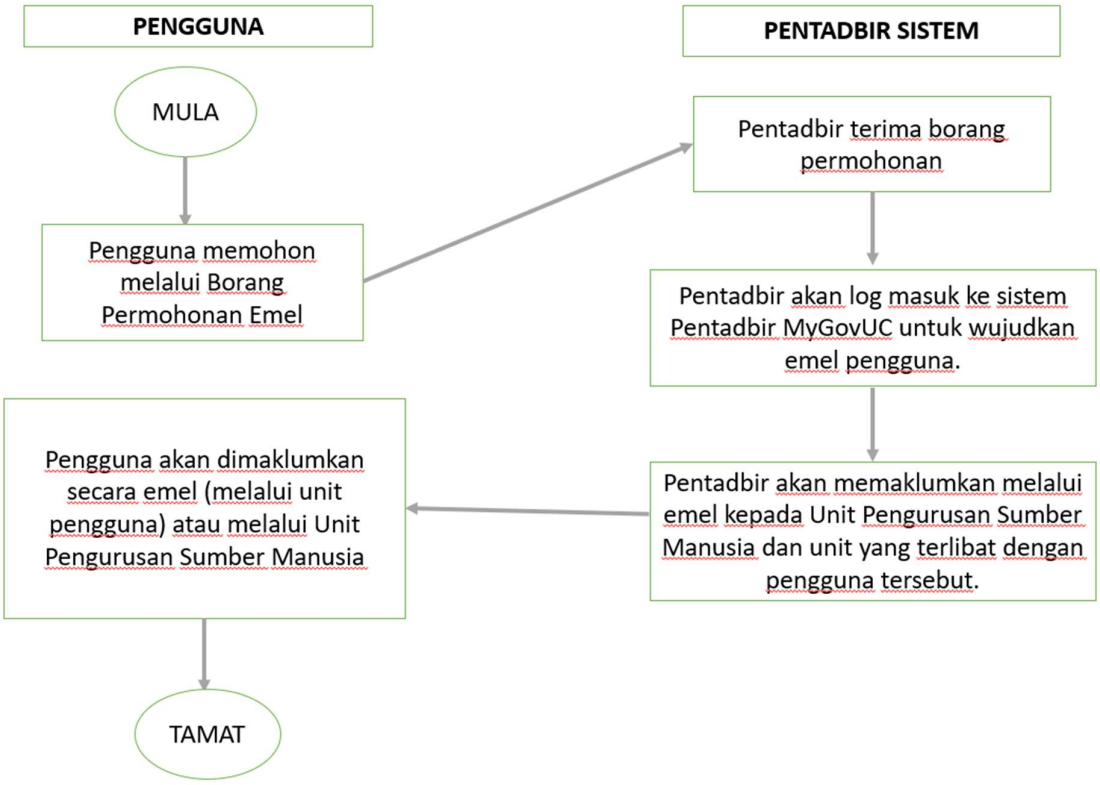
Nama:	No Tel:
Bahagian/Caw:	Lokasi Pejabat:
ID:	Password:
E-mel:	Alamat:

Peringatan:

1. Emel yang disediakan hendaklah digunakan untuk tujuan rasmi sahaja.
2. Setiap pengguna dikehendaki menukar katalaluan yang baru kepada 12 aksara gabungan huruf besar, huruf kecil, nombor dan simbol.
3. Setiap penguna dilarang daripada menggunakan emel APAD untuk tujuan lain seperti menyedia dan menghantar maklumat berulang-ulang atau yang boleh menjatuhkan imej Kerajaan.
4. Kegagalan mematuhi kepada perkara tersebut di atas membolehkan Tuan/Puan diambil tindakan.

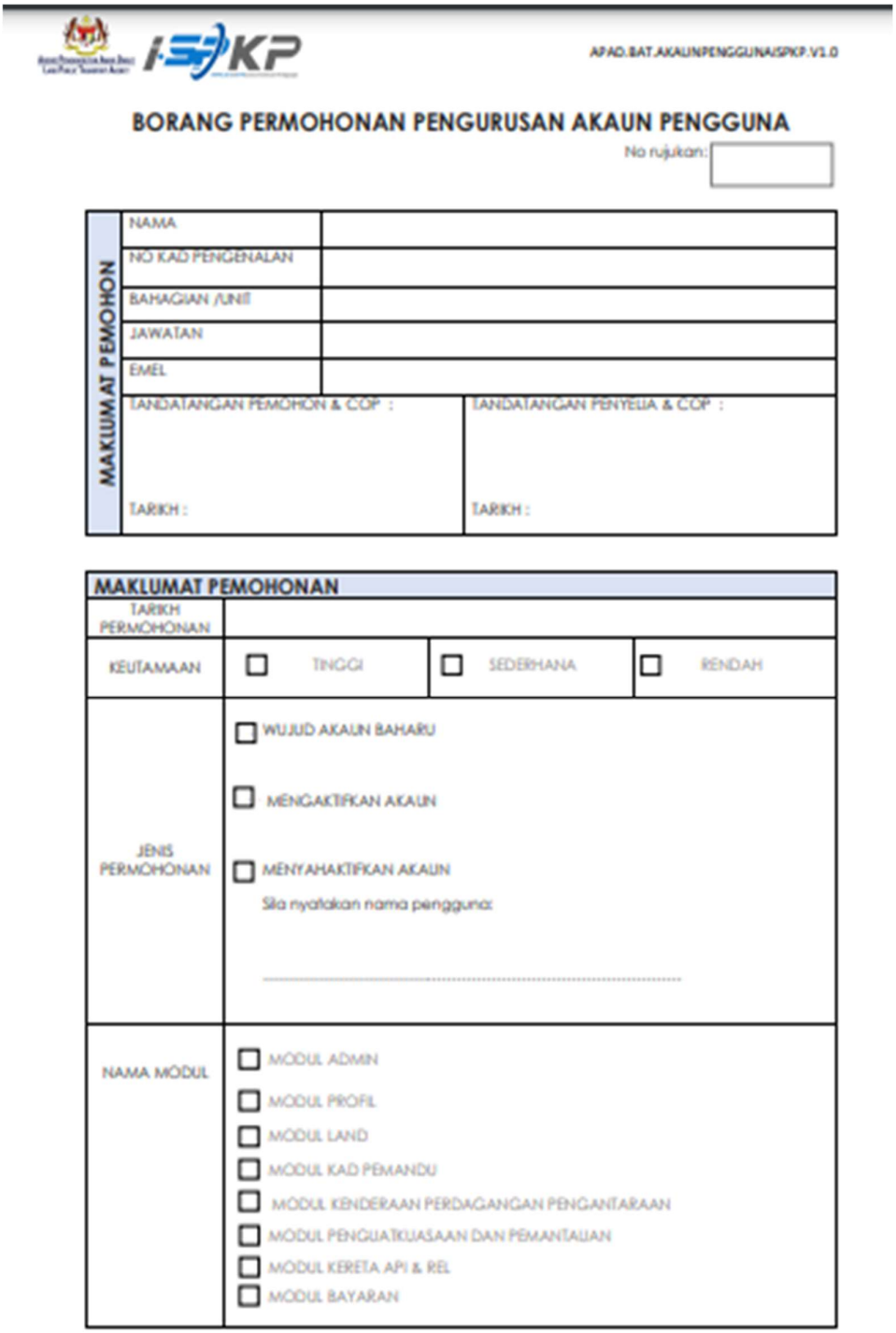
LAMPIRAN 6

PROSES KELULUSAN PENDAFTARAN E-MEL RASMI



LAMPIRAN 7

BORANG PENDAFTARAN CAPAIAN SISTEM PELESENAN KENDERAAN PERDAGANGAN (I-SPKP) APAD



APAD.BAT.AKAUNPENGGUNA/SPKP.V1.0

BORANG PERMOHONAN PENGURUSAN AKAUN PENGGUNA

No rujukan:

MAKLUMAT PEMOHON		
	NAMA	
	NO KAD PENGENALAN	
	BAHAGIAN /UNIT	
	JAWATAN	
	EMEL	
	TANDATANGAN PEMOHON & COP : TARIKH :	TANDATANGAN PENYELIA & COP : TARIKH :

MAKLUMAT PEMOHONAN			
TARIKH PERMOHONAN			
KEUTAMAAN	☐ TINGGI	☐ SEDERHANA	☐ RENDAH
JENIS PERMOHONAN	☐ WUJUD AKAUN BAHARU ☐ MENGAKTIFKAN AKAUN ☐ MENYAHAKTIFKAN AKAUN Sila nyatakan nama pengguna:		
NAMA MODUL	☐ MODUL ADMIN ☐ MODUL PROFIL ☐ MODUL LAND ☐ MODUL KAD PEMANDU ☐ MODUL KENDERAAN PERDAGANGAN PENGANTARAAN ☐ MODUL PENGUATKUASAAN DAN PEMANTAUAN ☐ MODUL KERETA API & REL ☐ MODUL BAYARAN		

	☐ MODUL TERMINAL ☐ MODUL MESYUARAT ☐ MODUL LINTAS SEMPADAN ☐ MODUL APLIKASI MOBIL ☐ MODUL PERMOHONAN PERKHIDMATAN ☐ MODUL PAPAN PEMUKA ☐ LAIN – LAIN sila nyatakan .....
PERINGKAT PENGGUNA	☐ PROCESS OFFICER (PO) ☐ VERIFICATION OFFICER 1 (VO1) ☐ VERIFICATION OFFICER 2 (VO2) ☐ VIEWER

PENGESAHAN (UNTUK KEGUNAAN PIHAK BAT)	
DISIAPKAN OLEH TANDATANGAN & COP : TARIKH:	DISAHKAN OLEH : TANDATANGAN & COP : TARIKH:

POLISI KESELAMATAN SIBER

PKS VERSI 1.0

apad secure

AGENSI PENGANGKUTAN AWAM DARAT