PELAN KESELAMATAN SIBER MARA

VERSI 2.0

Bahagian Teknologi Maklumat MARA

PELAN KESELAMATAN SIBER MARA
Versi 2.0

BAHAGIAN TEKNOLOGI MAKLUMAT MARA
Tingkat 6 & 7, Ibu Pejabat MARA
No. 21, Jalan MARA
50609 Kuala Lumpur
Tel: 03-261 32552 / 32562
Faks: 03-2698 6140
Emel: infobtm@mara.gov.my
Helpdesk:helpdesk@mara.gov.my

Reka bentuk:
Bahagian Teknologi Kreatif dan Multimedia

Diterbitkan oleh:
MAJLIS AMANAH RAKYAT (MARA)
No. 21, Jalan MARA, 50609 Kuala Lumpur.
Tel: 03-261 32552 / 32562
Faks: 03-26986140
Website: http://www.mara.gov.my

Kata Aluan Ketua Pengarah MARA

Saya mengucapkan rasa syukur ke hadrat Allah SWT serta syabas dan tahniah kepada Bahagian Teknologi Maklumat (BTM) atas inisiatif semakan dan menerbitkan semula Buku Pelan Keselamatan Siber MARA.

Pelan Keselamatan Siber MARA diwujudkan bagi menyokong Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) yang dikendalikan oleh Agensi Keselamatan Siber Negara di bawah Majlis Keselamatan Negara, Jabatan Perdana Menteri. Pelan ini bertujuan menjamin kesinambungan urusan MARA dalam menangani ancaman keselamatan siber secara komprehensif dan meminimumkan kesan daripada insiden keselamatan ICT.

Warga kerja MARA perlu memastikan langkah yang digariskan dalam Pelan Keselamatan Siber ini difahami, dipatuhi dan dilaksanakan dengan berkesan. Melalui Pelan Keselamatan Siber MARA ini juga, warga kerja MARA perlu sedar bahawa peranan dan tanggungjawab dalam melindungi aset ICT MARA amat penting bagi menjamin keberkesanan urusan MARA sama ada di peringkat dalaman atau membabitkan orang awam.

Bersamalah kita menyempurnakan tanggungjawab sebagai warga kerja MARA dalam usaha memastikan perkhidmatan Kerajaan khususnya di MARA lebih maju, efisien dan selamat.

Sekian dan selamat maju jaya.

DATO' AZHAR BIN ABDUL MANAF
Ketua Pengarah
MARA

Kata Aluan Timbalan Ketua Pengarah (Khidmat Pengurusan) / Ketua Pegawai Maklumat (CIO) MARA

Saya mengucapkan rasa syukur ke hadrat Allah SWT kerana dengan izin-Nya usaha untuk menyediakan Buku Pelan Keselamatan Siber MARA telah berjaya dilaksanakan.

Adalah menjadi hasrat MARA untuk meningkatkan keberkesanan sistem penyampaian melalui penggunaan teknologi ICT sejajar dengan peningkatan penggunaan teknologi. Walau bagaimanapun, dalam pelaksanaan tersebut, terdapat ancaman keselamatan siber seperti pencerobohan dan penipuan data. Oleh itu adalah menjadi tanggungjawab MARA dalam menangani perkara ini. Warga kerja MARA perlu memahami dan mengetahui kaedah penggunaan dan seterusnya bertanggungjawab mengurangi risiko ancaman keselamatan ICT.

Buku Pelan Keselamatan Siber ini menyediakan langkah keselamatan yang perlu dipatuhi oleh seluruh warga kerja MARA. Pematuhan kepada peraturan keselamatan seperti terkandung dalam buku ini adalah sebagai langkah keselamatan untuk menghalang sebarang pencerobohan kepada keselamatan ICT.

Tahniah dan terima kasih saya ucapkan kepada semua yang terlibat dalam penerbitan buku ini.

Sekian dan selamat maju jaya.

ROHAYAH BINTI MOHD ZAIN
Ketua Pegawai Maklumat (CIO)
MARA

ISI KANDUNGAN

PENGENALAN

OBJEKTIF

PERNYATAAN DASAR

SKOP

PRINSIP-PRINSIP

PENILAIAN RISIKO KESELAMATAN ICT

PENGENALAN

Pelan Keselamatan Siber (PKS) MARA mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Pelan ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MARA.

OBJEKTIF

Pelan Keselamatan Siber MARA diwujudkan untuk:

a) Menjamin kesinambungan urusan MARA dengan meminimumkan kesan insiden keselamatan ICT;
b) Memudahkan perkongsian maklumat sesuai dengan keperluan operasi MARA dengan memastikan semua aset ICT dilindungi;
c) Memastikan kelancaran operasi MARA dan meminimumkan kerosakan atau kemusnahan;
d) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
e) Mencegah salah guna atau kecurian aset ICT MARA;
f) Menimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
g) Meningkatkan tahap kesedaran keselamatan ICT kepada kakitangan, pengguna dan pembekal; dan
h) Memperkukuhkan pengurusan risiko.

PERNYATAAN PELAN

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

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

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan khususnya MARA dari capaian tanpa kuasa yang sah;
b) Menjamin setiap maklumat adalah tepat dan sempurna;
c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d) Memastikan akses kepada hanya pengguna-penggunayang sah atau penerimaan maklumat dari sumber yang sah.

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

a) Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang

dibenarkan

c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan
e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain 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.

SKOP

Aset ICT MARA terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan *personnel*. Pelan Keselamatan Siber MARA menetapkan keperluan-keperluan asas berikut:

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

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

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

a) Perkakasan
Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan MARA. Contohnya komputer, pelayan, peralatan komunikasi dan sebagainya;

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

c) Media storan
Semua media storan yang berkaitan seperti storan mudah alih, *catridge*, CD-ROM, pita cakera, pemacu cakera, pemacu pita, storan awan *(cloud storage)* dan lain-lain;

d) Perkhidmatan

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

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

e) Data atau Maklumat

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

f) Manusia

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

g) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara a) - f) di atas.

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Pelan Keselamatan Siber MARA dan perlu dipatuhi adalah seperti berikut:

a) Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat mengikut kehendak Arahan Keselamatan (Semakan dan Pindaan 2017) perenggan 18, muka surat 14;

b) Hak akses minimum

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

c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini 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.

d) Pengasingan

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 dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

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

f) Pematuhan

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

g) Pemulihan

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

h) Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

MARA hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin

meningkat hari ini. Justeru itu MARA perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat MARA 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.

MARA bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Arahan Keselamatan (Semakan dan Pindaan 2017), Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam dan Surat Pekeliling Am MARA Bilangan 2 Tahun 2018: Pelaksanaan Pengurusan Risiko MARA.

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

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

BIDANG 01: PEMBANGUNAN DAN PENYELENGGARAAN PELAN

PKSMARA - 0101 Pelan Keselamatan Siber

PKSMARA - 010101 Pelaksanaan Pelan
PKSMARA - 010102 Penyebaran Pelan
PKSMARA - 010103 Penyelenggaraan Pelan
PKSMARA - 010104 Pengecualian Pelan

BIDANG 01:

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

PKSMARA - 0101 Pelan Keselamatan Siber

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

PKSMARA - 010101 Pelaksanaan Pelan

Pelaksanaan pelan ini akan dijalankan oleh Ketua Pengarah MARA dibantu oleh Jawatankuasa Pemandu ICT (JPICT) MARA yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengawal Pusat.	Ketua Pengarah MARA, CIO, ICTSO dan semua Pengawal Pusat

PKSMARA - 010102 Penyebaran Pelan

Pelan ini perlu disebarkan kepada semua pengguna MARA (termasuk kakitangan, pembekal, pakar runding dan lain-lain) menggunakan *platform* yang boleh dicapai oleh pihak berkaitan seperti Laman Web Intra, Laman Web MARA, serahan *hardcopy*, e-mel dan lain-lain medium komunikasi.	ICTSO

PKSMARA - 010103 Penyelenggaraan Pelan

Pelan Keselamatan Siber MARA adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Pelan Keselamatan Siber MARA: a) Kenal pasti dan tentukan perubahan yang diperlukan; b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), MARA; c) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JPICT; dan d) Pelan ini hendaklah dikaji semula sekurang-kurangnya sekali dalam tempoh dua tahun atau mengikut keperluan semasa	ICTSO dan Pengurus ICT

PKSMARA - 010104 Pengecualian Pelan

Pelan Keselamatan Siber MARA adalah terpakai kepada semua pengguna ICT MARA dan tiada pengecualian diberikan.	Semua Pengguna

BIDANG 02: ORGANISASI KESELAMATAN

PKSMARA - 0201 Infrastruktur Organisasi Dalaman

PKSMARA - 020101 Ketua Pengarah MARA
PKSMARA - 020102 Ketua Pegawai Maklumat (CIO)
PKSMARA - 020103 Pegawai Keselamatan ICT (ICTSO)
PKSMARA - 020104 Pengurus ICT
PKSMARA - 020105 Pentadbir Sistem ICT
PKSMARA - 020106 Pengguna
PKSMARA - 020107 Jawatan Kuasa Keselamatan ICT MARA

PKSMARA - 0202 Pihak Ketiga

PKSMARA - 020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

---

BIDANG 02:

ORGANISASI KESELAMATAN

PKSMARA - 0201 Infrastruktur Organisasi Dalaman

Objektif:
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Pelan Keselamatan Siber MARA.

PKSMARA - 020101 Ketua Pengarah MARA

Ketua Pengarah MARA adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut:

Ketua Pengarah MARA

a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Pelan Keselamatan Siber MARA;

b) Memastikan semua pengguna mematuhi Pelan Keselamatan Siber MARA;

c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi;

d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Pelan Keselamatan Siber MARA; dan

e) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), MARA.

PKSMARA - 020102 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) bagi MARA ialah Timbalan Ketua Pengarah (Khidmat Pengurusan) MARA. CIO

Peranan dan tanggungjawab CIO adalah seperti berikut:

a) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;

b) Menentukan keperluan keselamatan ICT;

c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan Pelan Keselamatan Siber MARA serta pengurusan risiko dan pengauditan; dan

d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MARA.

PKSMARA - 020103 Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT (ICTSO) bagi MARA ialah Pengarah Bahagian Teknologi Maklumat (BTM), MARA. ICTSO

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

a) Menyedia, melaksana dan mengurus keseluruhan program-program keselamatan ICT MARA;

b) Menguatkuasakan pelaksanaan Pelan Keselamatan Siber MARA;

c) Memberi penerangan dan pendedahan berkenaan Pelan Keselamatan Siber MARA kepada semua pengguna;

d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Pelan Keselamatan Siber MARA;

e) Menjalankan pengurusan risiko;

f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MARA berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti *virus* dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

h) Melaporkan insiden keselamatan ICT kepada pihak Agensi Keselamatan Siber Negara (NACSA), memaklumkannya kepada CIO dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden seumpamanya dapat dielakkan;

i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;

j) Memberikan kebenaran hak akses yang berkaitan keselamatan ICT kepada pengguna; dan

k) Bertindak sebagai kordinator dan melaporkan insiden keselamatan ICT kepada CIO bagi insiden ICT berdasarkan Pelan Pemulihan Bencana (DRP).

PKSMARA - 020104 Pengurus ICT

Pengurus ICT bagi MARA ialah Timbalan Pengarah, Bahagian Teknologi Maklumat (BTM), MARA. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: Pengurus ICT

a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MARA;

b) Menentukan kawalan akses pengguna terhadap aset ICT MARA;

c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO;

d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MARA;

e) Membangun, mengkaji semula dan mengemas kini Pelan Pemulihan Bencana (DRP) keselamatan ICT;

f) Memastikan Pelan Keselamatan Siber MARA dikemas kini sesuai dengan perubahan teknologi, perubahan dasar kerajaan dan ancaman-ancaman terkini dari semasa ke semasa; dan

g) Memastikan Pelan Strategik ICT MARA mengandungi inisiatif di dalam aspek keselamatan ICT.

PKSMARA - 020105 Pentadbir Sistem ICT

Pentadbir Sistem ICT bagi MARA ialah Ketua Pegawai Teknologi Maklumat/Pegawai Teknologi Maklumat, Bahagian Teknologi Maklumat (BTM), dan gred F tertinggi di pusat MARA. Pentadbir Sistem ICT

a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang 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 Pelan Keselamatan Siber MARA;

c) Memantau aktiviti capaian harian sistem aplikasi pengguna;

d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;

e) Menganalisis dan menyimpan rekod jejak audit;

f) Menyediakan laporan mengenai aktiviti capaian secara berkala;

g) Memastikan setiap pengguna dikenali dengan menggunakan *User ID* yang unik; dan

h) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.

Pentadbir Sistem bertanggungjawab sepanjang menjalankan fungsi-fungsi berikut;

Pentadbir Rangkaian Dan Keselamatan

a) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di MARA beroperasi sepanjang masa;

b) Memastikan semua peralatan dan perisian rangkaian diselenggara dengan sempurna;

c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;

d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;

e) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian;

f) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan sambungan rangkaian selainnya perlu mendapat kelulusan ICTSO;

g) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; dan

h) Melibatkan diri dalam sebarang aktiviti penilaian tahap keselamatan ICT *(Security Posture Assessment)* serta penilaian risiko keselamatan maklumat.

Pentadbir Pangkalan Data

a) Melaksanakan instalasi dan menambah baik pangkalan data serta perisian lain yang berkaitan dengan pangkalan data;

b) Memastikan pangkalan data boleh digunakan pada setiap masa;

c) Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data;

d) Melaksanakan *data masking* dalam menyediakan data latihan;

e) Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur;

f) Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip Pelan Keselamatan Siber;

g) Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data;

h) Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO; dan

i) Melibatkan diri dalam sebarang aktiviti penilaian tahap keselamatan ICT *(Security Posture Assessment)* serta penilaian risiko keselamatan maklumat.

Pentadbir Laman Web

a) Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah;

b) Memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar;

c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman;

d) Mengehadkan capaian Pentadbir Laman Web bahagian ke *web server*;

e) Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal MARA;

f) Memastikan maklumat/data berklasifikasi rahsia rasmi (RAHSIA BESAR, RAHSIA, SULIT, TERHAD) tidak dibenarkan dicapai melalui laman web tanpa ada ciri-ciri keselamatan yang khusus pada laman web berkenaan. Laman web hanya untuk paparan maklumat rasmi sahaja;

g) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi;

h) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*;

i) Melaksanakan proses *backup* dan *restoration* secara berkala; dan

j) Melaporkan sebarang pelanggaran keselamatan laman portal kepada ICTSO.

Pentadbir Pusat Data

a) Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat;

b) Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data;

c) Menjadual dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala;

d) Melaksanakan Pelan Pemulihan Bencana (DRP) mengikut prinsip Pengurusan Kesinambungan Perkhidmatan dalam Pelan Keselamatan Siber;

e) Melaksanakan prinsip-prinsip Pelan Keselamatan Siber;

f) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan; dan

g) Melibatkan diri dalam setiap aktiviti penilaian tahap keselamatan ICT *(Security Posture Assessment)* serta penilaian risiko keselamatan maklumat.

Pentadbir Sistem Aplikasi

a) Mengkaji cadangan pembangunan atau penyelarasan sistem atau modul di MARA;

b) Membuat kajian semula serta memperbaiki sistem atau modul sedia ada di MARA;

c) Membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem atau modul di MARA;

d) Membuat pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa;

e) Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem atau modul;

f) Menyediakan dokumentasi sistem atau modul dan manual pengguna;

g) Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas;

h) Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaanya;

i) Memastikan *virus pattern, hotfix* dan *patch* yang berkaitan dengan sistem aplikasi terkemaskini supaya terhindar daripada ancaman *virus* dan penggodam;

j) Mematuhi dan melaksanakan prinsip-prinsip Pelan Keselamatan Siber dalam pewujudkan akaun pengguna ke atas setiap sistem aplikasi;

k) Mengehadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya;

l) Melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya; dan

m) Melibatkan diri dalam sebarang aktiviti penilaian tahap keselamatan ICT *(Security Posture Assessment)* serta penilaian risiko keselamatan maklumat.

Pentadbir E-mel

a) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat;

b) Mengesah dan memaklumkan kepada ICTSO sekiranya terdapat insiden keselamatan melalui saluran rasmi;

c) Memastikan kemudahan membuat capaian e-mel diperolehi melalui pelbagai peralatan ICT dan alat komunikasi; dan

d) Memastikan pengguna e-mel MARA berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel dan Internet MARA serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan.

PKSMARA - 020106 Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti berikut: Pengguna

a) Membaca, memahami dan mematuhi Pelan Keselamatan Siber MARA;

b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;

c) Melepasi tapisan keselamatan (jika berkaitan);

d) Melaksanakan prinsip-prinsip Pelan Keselamatan Siber MARA dan menjaga kerahsiaan maklumat MARA;

e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;

f) Menghadiri program-program kesedaran mengenai keselamatan ICT;

g) Menandatangani Surat Akuan Pematuhan Pelan Keselamatan Siber MARA sebagaimana **Lampiran 1**.

h) Melaksanakan langkah-langkah perlindungan seperti berikut:

i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

iii) Menentukan maklumat sedia untuk digunakan;

iv) Menjaga kerahsiaan kata laluan;

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

vi) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;

vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; dan

viii) Mengawal aktiviti penggunaan media sosial seperti dibawah:

- Mengelakkan ketirisan maklumat;
- Tidak memberi atau mendedahkan sebarang komen atau pernyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan;

– Tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan

– Tidak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja.

PKSMARA - 020107 Jawatan Kuasa Keselamatan ICT MARA

Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MARA.

JKICT MARA

Jawatankuasa Pemandu ICT MARA (JPICT) juga berperanan sebagai JKICT MARA.

Keanggotaan JPICT dan JKICT MARA adalah seperti berikut:

Pengerusi : Ketua Pengarah MARA

Ahli / Pengerusi silih ganti : Timbalan Ketua Pengarah (Khidmat Pengurusan) – CIO MARA / Timbalan Ketua Pengarah/Pengarah Kanan

Ahli :

a) Pengarah/Timbalan Pengarah Pembangunan Usahawan;

b) Pengarah/Timbalan Pengarah Pendidikan Tinggi;

c) Pengarah/Timbalan Pengarah Perundangan;

d) Pengarah/Timbalan Pengarah Pengurusan Aset dan Perolehan;

e) Pengarah/Timbalan Pengarah Perancangan Strategik;

f) Pengarah/Timbalan Pengarah Kemahiran dan Teknikal;

g) Pengarah/Timbalan Pengarah Kewangan;

h) Pengarah/Timbalan Pengarah Pendidikan Menengah;

i) Pengarah/Timbalan Pengarah Infrastruktur Komersial;

j) Pengarah/Timbalan Pengarah Binaan dan Selenggaraan;

k) Pengarah/Timbalan Pengarah Teknologi Maklumat;

l) Pengarah/Timbalan Pengarah Pembiayaan Perniagaan;

m) Pengarah/Timbalan Pengarah Audit Dalam;

n) Ketua Unit Integriti; dan

o) Pegawai Keselamatan ICT *(ICT Security Officer)* MARA

Urus Setia : Bahagian Teknologi Maklumat

Korum : 5 orang (Pengerusi serta 4 ahli)

Bidang kuasa :

a) Memperakukan/meluluskan dokumen Pelan Keselamatan Siber MARA;

b) Memantau tahap pematuhan keselamatan ICT;

c) Memperakukan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MARA yang mematuhi keperluan Pelan Keselamatan Siber MARA;

d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;

e) Memastikan Pelan Keselamatan Siber MARA selaras dengan dasar-dasar ICT kerajaan semasa;

f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa;

g) Membincang tindakan yang melibatkan pelanggaran Pelan Keselamatan Siber MARA; dan

h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.

PKSMARA - 020108 PASUKAN TINDAK BALAS INSIDEN KESELAMATAN ICT (MARACERT)

ICTSO, MARACERT, Pentadbir Sistem ICT

Keanggotaan MARACERT adalah seperti berikut:

Pengerusi : Pegawai Keselamatan ICT (ICTSO)

Ahli :

a) Timbalan Pengarah Bahagian Teknologi Maklumat;

b) Ketua Pegawai Teknologi Maklumat/Pegawai Teknologi Maklumat Bahagian Teknologi Maklumat;

c) Pegawai Teknologi Maklumat Bahagian Pendidikan Menengah;

d) Pegawai Teknologi Maklumat Bahagian Pendidikan Tinggi; dan

e) Pegawai Teknologi Maklumat Bahagian Kemahiran Teknikal;

Urus setia : Bahagian Teknologi Maklumat

Peranan dan tanggungjawab MARACERT adalah seperti berikut:

a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;

b) Merekod dan menjalankan siasatan awal insiden yang diterima;

c) Menangani tindak balas *(response)* insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;

d) Menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan pihak NACSA sama ada sebagai *input* atau untuk tindakan seterusnya;

e) Merujuk agensi-agensi di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan;

f) Melaporkan sebarang maklumbalas dan insiden keselamatan ICT kepada JKICT;

g) Menasihati MARA dalam mengambil tindakan pemulihan dan pengukuhan; dan

h) Menyebarkan makluman berkaitan pengukuhan.

PKSMARA - 0202 Pihak Ketiga

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).

PKSMARA - 020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Bertujuan untuk memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal.

CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

Perkara yang perlu dipatuhi termasuk yang berikut:

a) Membaca, memahami dan mematuhi Pelan Keselamatan Siber MARA yang berkaitan;

b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;

c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;

d) Akses kepada aset ICT MARA perlu berlandaskan kepada perjanjian kontrak;

e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.

i. Pelan Keselamatan Siber MARA;

ii. Tapisan Keselamatan;

iii. Perakuan Akta Rahsia Rasmi 1972; dan

iv. Hak Harta Intelek.

(f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan Pelan Keselamatan Siber MARA sebagaimana **Lampiran 1.**

BIDANG 03: PENGURUSAN ASET

PKSMARA - 0301 Akauntabiliti Aset
PKSMARA - 030101 Inventori Aset ICT

PKSMARA - 0302 Pengelasan dan Pengendalian Maklumat
PKSMARA - 030201 Kategori Maklumat
PKSMARA - 030202 Pengelasan Maklumat
PKSMARA - 030203 Pengendalian Maklumat

BIDANG 03:

PENGURUSAN ASET

PKSMARA - 0301 Akauntabiliti Aset

Objektif:
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MARA.

PKSMARA - 030101 Inventori Aset ICT

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

Pentadbir Sistem ICT dan Semua Pengguna

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkodkan dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini;

b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;

c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MARA;

d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan

e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

PKSMARA - 0302 Pengelasan dan Pengendalian Maklumat

Objektif:
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

PKSMARA - 030201 Kategori Maklumat

Mengenal pasti kategori maklumat merupakan satu langkah penting dalam memastikan perlindungan yang mencukupi dan bersesuaian dengan kategori maklumat berkenaan.

Semua Pengguna

Semua maklumat yang dijana atau dikumpul oleh MARA hendaklah diasingkan mengikut kategori Maklumat Rasmi dan Maklumat Rahsia Rasmi.

Kedua-dua kategori boleh mengandungi *Personal Identifiable Information (PII)*.

Data Terbuka juga merupakan sebahagian daripada Maklumat Rasmi.

a) Maklumat Rahsia Rasmi
Maklumat Rahsia Rasmi mempunyai erti yang diberikan kepadanya di bawah Akta Rahsia Rasmi 1972 [Akta 88]. Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

b) Maklumat Rasmi
Maklumat Rasmi adalah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh mana-mana agensi Kerajaan semasa menjalankan urusan rasmi. Maklumat Rasmi ini juga adalah merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

c) Maklumat Pengenalan Peribadi
Maklumat Pengenalan Peribadi PII adalah maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu yang juga dikategorikan sebagai Maklumat Rahsia Rasmi.

d) Data Terbuka
Data Terbuka adalah maklumat yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi kerajaan dan organisasi swasta untuk pelbagai tujuan. MARA hendaklah mematuhi pekeliling yang sedang berkuat kuasa.
PII dikecualikan daripada Data Terbuka

PKSMARA - 030202 Pengelasan Maklumat

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan (Semakan dan Pindaan 2017) .

Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017) seperti berikut:
a) Rahsia Besar;
b) Rahsia;
c) Sulit; atau
d) Terhad.

Semua Pengguna

PKSMARA - 030203 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:

a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

c) Menentukan maklumat sedia untuk digunakan;

Semua Pengguna

d) Menjaga kerahsiaan kata laluan;

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

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

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

BIDANG 04: KESELAMATAN SUMBER MANUSIA

PKSMARA - 0401 Keselamatan Sumber Manusia Dalam Tugas Harian

PKSMARA - 040101 Sebelum Perkhidmatan
PKSMARA - 040102 Dalam Perkhidmatan
PKSMARA - 040103 Bertukar Atau Tamat Perkhidmatan

BIDANG 04:

KESELAMATAN SUMBER MANUSIA

PKSMARA - 0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:
Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan MARA, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga MARA hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

PKSMARA - 040101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MARA serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; — Semua Pengguna

b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MARA serta pihak ketiga yang terlibat seperti yang termaktub dalam Arahan Keselamatan (Semakan dan Pindaan 2017) selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan

c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

PKSMARA - 040102 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a) Memastikan pegawai dan kakitangan MARA serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MARA; — Semua Pengguna

b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MARA secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;

c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan MARA serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MARA; dan

d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Sumber Manusia, MARA.

PKSMARA - 040103 Bertukar Atau Tamat Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a) Memastikan semua aset ICT dikembalikan kepada pentadbiran Bahagian/Pusat semasa (sebelum berpindah) mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. — Semua Pengguna

b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan pemprosesan maklumat mengikut peraturan yang ditetapkan oleh MARA dan/atau terma perkhidmatan.

BIDANG 05: KESELAMATAN FIZIKAL DAN PERSEKITARAN

PKSMARA - 0501 Keselamatan Kawasan
PKSMARA - 050101 Kawalan Kawasan
PKSMARA - 050102 Kawalan Masuk Fizikal
PKSMARA - 050103 Kawasan Larangan
PKSMARA - 050104 Keselamatan Pusat Data
PKSMARA - 050105 Keselamatan Bilik *Server* dan Bilik Rangkaian

PKSMARA - 0502 Keselamatan Peralatan
PKSMARA - 050201 Perkakasan ICT
PKSMARA - 050203 Storan Awan (*Cloud Storage*)
PKSMARA - 050204 Media Tandatangan Digital
PKSMARA - 050205 Media Perisian dan Aplikasi
PKSMARA - 050206 Penyelenggaraan Perkakasan
PKSMARA - 050207 Peralatan di Luar Premis
PKSMARA - 050208 Pelupusan Perkakasan
PKSMARA - 050209 Pinjaman Perkakasan ICT

PKSMARA - 0503 Keselamatan Persekitaran
PKSMARA - 050301 Kawalan Persekitaran
PKSMARA - 050302 Bekalan Kuasa
PKSMARA - 050303 Kabel
PKSMARA - 050304 Prosedur Kecemasan
PKSMARA - 050305 Mekanisme Kawalan Peralatan/Perisian Kawalan Peralatan Sewaan/Ujicuba (*Proof of Concept*)

PKSMARA - 0504 Keselamatan Dokumen
PKSMARA - 050401 Dokumen

BIDANG 05:

KESELAMATAN FIZIKAL DAN PERSEKITARAN

PKSMARA - 0501 Keselamatan Kawasan

Objektif:
Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

PKSMARA - 050101 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

Pengarah Bahagian Pengurusan Aset dan Perolehan, Pengarah Bahagian Pengurusan Risiko dan Inspektorat, CIO dan ICTSO

a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;

b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;

c) Memasang alat penggera atau kamera;

d) Mengehadkan jalan keluar masuk;

e) Mengadakan kaunter kawalan;

f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat;

g) Mewujudkan perkhidmatan kawalan keselamatan;

h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;

i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;

j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;

k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad;

l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya;

m) Memastikan butiran pelawat yang keluar masuk ke kawasan larangan direkodkan;

n) Memastikan pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; dan

o) Memastikan lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam.

PKSMARA - 050102 Kawalan Masuk Fizikal

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a) Setiap pengguna MARA hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;

Semua Pengguna

b) Semua pas keselamatan hendaklah diserahkan balik kepada MARA apabila pengguna berhenti atau bersara;

c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter utama. Amalan ini juga perlu dipatuhi di semua pusat MARA. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan

d) Kehilangan pas mestilah dilaporkan dengan segera.

PKSMARA - 050103 Kawasan Larangan

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.

Pentadbir Sistem ICT

a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan

b) 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 di iringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.

PKSMARA - 050104 Keselamatan Pusat Data

Untuk memastikan semua *server* sentiasa selamat daripada pencerobohan atau sebarang ancaman dan membolehkan ia dicapai sepanjang masa, semua *server* hendaklah diletakkan di dalam pusat data yang mempunyai kemudahan keselamatan, penyaman udara khas dan kemudahan perlindungan suhu dan kebakaran.

Pentadbir Sistem ICT

Pusat Data juga seharusnya dilengkapkan dengan ciri-ciri keselamatan lain seperti CCTV dan UPS. Berikut adalah beberapa langkah untuk melindungi *server* tersebut :

a) Memantau dan mengawal keluar masuk pengguna ke pusat data melalui sistem *Security Access Door* atau berkunci dan CCTV;

b) Memastikan hanya pegawai-pegawai yang mempunyai kebenaran sahaja yang dibenarkan memasuki Pusat Data;

c) Memastikan Pusat Data sentiasa bersih dan peralatan ICT tidak terdedah kepada habuk;

d) Memastikan penyaman udara berfungsi dengan baik dan suhunya adalah bersesuaian dengan Pusat Data;

e) Memastikan semua peralatan keselamatan, UPS dan penyaman udara diselenggarakan secara berkala;

f) Memastikan Pusat Data dilengkapi dengan Sistem Pencegahan dan Penggera Kebakaran yang diselenggara secara berkala; dan

g) Memastikan tiada sebarang foto diambil di Pusat Data.

PKSMARA - 050105 Keselamatan Bilik *Server* dan Bilik Rangkaian

Bilik *Server* adalah bilik yang menempatkan *server* dan peralatan rangkaian serta keselamatan dengan skala dan saiz yang lebih kecil dari Pusat Data MARA. Pusat-pusat operasi MARA seperti Institusi Pendidikan MARA (IPMa) dan Pejabat MARA Negeri (PMN) lazimnya mempunyai Bilik *Server* berbanding Pusat Data di Ibu Pejabat MARA.

Pentadbir Sistem ICT

Manakala Bilik Rangkaian atau sudut peralatan rangkaian adalah lokasi dimana diletakkan rak rangkaian (mengandungi perkakasan rangkaian) sama ada *wall standing* atau *wall mounted* (digantung).

Diantara beberapa langkah keselamatan yang perlu diambil termasuklah:

a) Memastikan sistem penyaman udara untuk perlindungan suhu disediakan dalam Bilik *Server*/ Rangkaian berkenaan. Bagi bilik yang memuatkan perkakasan rangkaian *wall mounted* perlu mempunyai kitar pengudaraan yang bersesuaian.

b) Memastikan sistem pencegahan kebakaran disediakan di bangunan yang mana Bilik *Server* ditempatkan;

c) Memastikan keperluan UPS sekurang-kurangnya mampu melindungi *Server* dan perkakasan rangkaian yang utama;

d) Memantau dan mengawal keluar masuk pengguna ke Bilik *Server* dengan menyediakan Buku Log Pelawat;

e) Memastikan hanya pegawai-pegawai yang mempunyai kebenaran sahaja yang dibenarkan memasuki Bilik *Server*;

f) Memastikan Bilik *Server* sentiasa bersih dan peralatan ICT tidak terdedah kepada habuk;

g) Memastikan penyaman udara mestilah berfungsi dengan baik, di mana suhunya adalah bersesuaian dengan Bilik *Server*;

h) Menyelenggara semua peralatan keselamatan, UPS dan penyaman udara secara berkala;

i) Memastikan rak pekakasan *server* dan rangkaian tidak diletakkan di bawah penghawa dingin, tingkap atau ruang-ruang yang terbuka pada persekitaran luar;

j) Memastikan tiada sebarang perkakasan lain diletakkan di bawah rak *wall mounted* bagi memastikan rak tersebut boleh dicapai pada bila-bila masa; dan

k) Memastikan setiap rak perkakasan *server* dan rangkaian dikunci dan kunci disimpan di tempat yang selamat.

PKSMARA - 0502 Keselamatan Peralatan

Objektif:

Melindungi peralatan ICT MARA dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

PKSMARA - 050201 Perkakasan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Semua Pengguna, Pentadbir Sistem ICT

a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;

b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;

e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

f) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan. Setiap komputer pentadbiran perlu *Join Domain* untuk membolehkan akaun pada *Active Directory* MARA digunakan sebagai log masuk;

h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply (UPS)*;

j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

l) Peralatan ICT yang hendak dibawa keluar dari premis MARA, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;

m) Peralatan ICT yang hilang hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa dari semasa ke semasa;

n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT atau *Helpdesk* BTM untuk dibaik pulih;

q) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

r) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT;

s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

t) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan *"OFF"* apabila meninggalkan pejabat;

u) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO;

v) Memastikan plug dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya; dan

w) Sebarang pelekat selain bagi tujuan tidak rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik.

PKSMARA - 050202 Media Storan

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, cakera keras, pita magnetik, *optical disk, flash disk, thumb drive* dan media storan lain.

Semua Pengguna

Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;

b) Penggunaan media storan elektronik bagi penyimpanan maklumat-maklumat rahsia rasmi untuk tujuan dibawa keluar hendaklah mematuhi perenggan 138 Arahan Keselamatan (Semakan dan Pindaan 2017);

c) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;

d) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;

e) Semua salinan 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;

f) Akses dan pergerakan media storan hendaklah direkodkan;

g) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal;

h) Mengadakan salinan atau penduaan *(backup)* pada media storan bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;

i) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat;

j) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.

k) Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu mengikut Garis Panduan Sanitasi Media Sektor Awam;

l) Perkakasan *backup* (CD/DVD *duplicator*) hendaklah diletakkan di tempat yang lebih selamat dan terhad kepada pengguna yang dibenarkan sahaja; dan

m) Sebarang kehilangan media storan yang berlaku hendaklah dilaporkan mengikut Prosedur Pelaporan Insiden.

PKSMARA - 050203 Storan Awan *(Cloud Storage)*

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Memastikan tiada sebarang maklumat rahsia rasmi disimpan pada storan awan awam *(public cloud storage)* seperti *Dropbox* ,*Google Drive* dan sebagainya sepertimana yang dinyatakan dalam Arahan Keselamatan (Semakan dan Pindaan 2017) perenggan 139; — Semua Pengguna

b) Memastikan setiap dokumen rasmi tidak disimpan di storan awan awam *(public cloud storage)*;

c) Memastikan pengguna tidak menyimpan dokumen tidak rasmi dan tidak berkaitan seperti yang berbentuk hiburan dan tidak bermanfaat pada storan awan yang disediakan oleh MARA;

d) Memastikan kandungan storan awan yang disediakan oleh MARA diurus dengan baik dan sentiasa membuat kerja-kerja pengemaskinian data atau *housekeeping* dari semasa ke semasa; dan

e) Memastikan perkongsian fail dan *folder* hanya dibuat untuk pengguna yang dibenarkan sahaja.

PKSMARA - 050204 Media Tandatangan Digital

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Semua Pengguna

a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;

b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan

c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.

PKSMARA - 050205 Media Perisian dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Semua Pengguna

a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MARA;

b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT;

c) Lesen perisian *(registration code, serials, CD-keys)* perlu disimpan berasingan daripada *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan

d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

PKSMARA - 050206 Penyelenggaraan Perkakasan

Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. — Pegawai Aset dan Pentadbir Sistem ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan;

b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;

d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;

e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan

f) Penyelenggaraan perkakasan oleh pembekal perlu dilakukan secara *onsite* dengan pengawasan oleh pihak yang berkenaan. *Remote access* adalah tidak dibenarkan; dan

g) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.

PKSMARA - 050207 Peralatan di Luar Premis

Perkakasan yang dibawa keluar dari premis MARA adalah terdedah kepada pelbagai risiko.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Semua Pengguna

a) Peralatan perlu dilindungi dan dikawal sepanjang masa;

b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian;

c) Sebarang sambungan ke rangkaian dan Internet di tempat awam perlu mengambilkira faktor keselamatan rangkaian terutamanya melibatkan urusan kerja rasmi;

d) Perkakasan perlu dipastikan tidak digunakan mana-mana pihak ketiga;

e) Pergerakan aset perlu melalui prosedur yang ditetapkan berserta borang yang berkaitan dan direkodkan bagi tujuan pemantauan; dan

f) Sebarang laporan kehilangan peralatan hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa dari semasa ke semasa.

PKSMARA - 050208 Pelupusan Perkakasan

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MARA dan ditempatkan di MARA.

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MARA.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

Semua, Pegawai Aset dan Bahagian Teknologi Maklumat

a) Semua pemusnahan peralatan khususnya yang mengandungi maklumat rahsia rasmi hendaklah mengikut peraturan yang ditetapkan oleh Kerajaan sepertimana yang disebutkan dalam perenggan 144 Arahan Keselamatan (Semakan dan Pindaan 2017). Prosedur pemusnahan tersebut boleh merujuk kepada Garis Panduan Sanitasi Media Sektor Awam ;

b) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

c) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

d) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

e) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Harta MARA;

f) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat atau tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

g) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut :

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM, hardisk, motherboard* dan sebagainya;

ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MARA;

iii. Memindah keluar dari MARA mana-mana peralatan ICT yang hendak dilupuskan;

iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MARA; dan

v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

PKSMARA - 050209 Pinjaman Perkakasan ICT

Semua peralatan ICT yang dipinjam dari BTM/ pusat lain atau dibawa keluar atau masuk perlulah dipastikan perkara berikut; — Semua Pengguna

a) Memastikan makluman peminjam dan peralatan dipinjam direkodkan ketika peminjaman dan pemulangan dibuat;

b) Memastikan tempoh pinjaman dihadkan kepada tempoh masa yang dipersetujui dan tidak terlalu lama tempohnya;

c) Melaporkan sebarang kerosakan dan kegagalan peralatan berfungsi dengan baik kepada *Helpdesk*/Pentadbir Sistem ICT dengan kadar segera; dan

d) Sebarang laporan kehilangan peralatan pinjaman hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa dari semasa ke semasa.

PKSMARA - 0503 Keselamatan Persekitaran

Objektif:

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

PKSMARA - 050301 Kawalan Persekitaran

Semua Pengguna

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 Teknologi Maklumat (BTM) MARA, Bahagian Aset dan Perolehan (BAP) MARA, Bahagian Binaan dan Senggaraan (BBS) MARA dan Bahagian Pengurusan Risiko dan Inspektorat (BPIN) MARA.

Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi:

a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;

b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;

c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;

d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;

e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;

f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;

g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan

h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.

PKSMARA - 050302 Bekalan Kuasa

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;

b) 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

c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.

Bahagian Teknologi Maklumat, Bahagian Aset dan Perolehan, Pengawal Pusat Luar Ibu Pejabat dan ICTSO

PKSMARA - 050303 Kabel

Kabel rangkaian hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah.

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;

b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;

c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.

Bahagian Teknologi Maklumat, MARA dan ICTSO

PKSMARA - 050304 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Pengurusan Keselamatan Perlindungan 2015; dan

b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai MERT MARA yang dilantik mengikut pusat.

Semua Pengguna

PKSMARA - 050305 Mekanisme Kawalan Peralatan/Perisian Kawalan Peralatan Sewaan/Ujicuba (*Proof of Concept*)

Sebarang *proof of concept (POC)* yang dijalankan perlu mendapatkan kelulusan ICTSO dengan mengambilkira perkara-perkara berikut: — Pentadbir Sistem ICT dan ICTSO

a) Penerimaan

i. Peralatan/perisian yang diterima bebas daripada sebarang *malware* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT MARA.

ii. Pembekal yang terlibat perlu memastikan semua syarat keselamatan dipatuhi:

- Pelan Keselamatan Siber MARA;
- Perakuan Akta Rahsia Rasmi 1972; dan
- Hak Harta Intelek.

b) Penyelenggaraan

i. Capaian melalui rangkaian luar MARA adalah tidak dibenarkan; dan

ii. Aktiviti penyelenggaraan adalah di bawah pengawasan pegawai MARA.

c) Pemulangan

i. Maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*secured delete*); dan

ii. Memastikan semua maklumat tidak tertinggal pada peralatan/perisian.

d) Hasil penemuan atau laporan hasil dari POC perlu diserahkan dan dibentang kepada pihak MARA dan tidak dibenarkan untuk disebarkan atau dikongsi dengan mana-mana pihak luar.

PKSMARA - 0504 Keselamatan Dokumen

Objektif:

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

PKSMARA - 050401 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Semua Pengguna

a) Setiap dokumen hendaklah ditanda dan dilabelkan mengikut peringkat keselamatan seperti Rahsia Besar, Rahsia, Sulit atau Terhad;

b) Memastikan kaedah penyimpanan dokumen selaras dengan Arahan Keselamatan (Semakan dan Pindaan 2017);

c) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur Arahan Keselamatan (Semakan dan Pindaan 2017);

d) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan (Semakan dan Pindaan 2017);

e) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan (Semakan dan Pindaan 2017), Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara;

f) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik;

g) Memastikan cetakan yang mengandungi maklumat rahsia rasmi diambil segera dari pencetak;

h) Sistem penyimpanan dokumentasi perlu mempunyai ciri-ciri keselamatan; dan

i) Semua aktiviti capaian dokumentasi sedia ada perlu dikawal atau direkodkan.

BIDANG 06: PENGURUSAN OPERASI DAN KOMUNIKASI

PKSMARA - 0601 Pengurusan Prosedur Operasi
PKSMARA - 060101 Pengendalian Prosedur
PKSMARA - 060102 Kawalan Perubahan
PKSMARA - 060103 Pengasingan Tugas dan Tanggungjawab
PKSMARA - 060104 Prosedur Pengurusan Insiden

PKSMARA - 0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga
PKSMARA - 060201 Perkhidmatan Penyampaian

PKSMARA - 0603 Perancangan dan Penerimaan Sistem
PKSMARA - 060301 Perancangan Kapasiti
PKSMARA - 060302 Penerimaan Sistem

PKSMARA - 0604 Perisian Berbahaya
PKSMARA - 060401 Perlindungan dari Perisian Berbahaya
PKSMARA - 060402 Perlindungan dari *Mobile Code*

PKSMARA - 0605 *Housekeeping*
PKSMARA - 060501 *Backup*

PKSMARA - 0606 Pengurusan Rangkaian
PKSMARA - 060601 Kawalan Infrastruktur Rangkaian

PKSMARA - 0607 Pengurusan Media
PKSMARA - 060701 Penghantaran dan Pemindahan
PKSMARA - 060702 Prosedur Pengendalian Media
PKSMARA - 060703 Keselamatan Sistem Dokumentasi

PKSMARA - 0608 Pengurusan Pertukaran Maklumat
PKSMARA - 060801 Pertukaran Maklumat
PKSMARA - 060802 Pengurusan Mel Elektronik (*E-mel*)

PKSMARA - 0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)
PKSMARA - 060901 E-Dagang
PKSMARA - 060902 Maklumat Umum

PKSMARA - 0610 Pemantauan
PKSMARA - 061001 Pengauditan dan Forensik ICT
PKSMARA - 061002 Jejak Audit
PKSMARA - 061003 Sistem Log
PKSMARA - 061004 Pemantauan Log

BIDANG 06:

PENGURUSAN OPERASI DAN KOMUNIKASI

PKSMARA - 0601 Pengurusan Prosedur Operasi

Objektif:
Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

PKSMARA - 060101 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Semua Pengguna

a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal;

b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan

c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan

PKSMARA - 060102 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Semua Pengguna

a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;

b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;

c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan

d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

PKSMARA - 060103 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Pengurus ICT dan ICTSO

a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;

b) Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan

c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

PKSMARA - 060104 Prosedur Pengurusan Insiden

MARACERT menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari pihak NACSA atau laporan dari sumber lain. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden dengan Keutamaan 2 (Merah) perlu dimaklumkan kepada pihak NACSA. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguatkuasa undang-undang.

MARACER, ICTSO dan Pentadbir Sistem ICT

MARACERT yang diketuai oleh ICTSO akan menjalankan tindakan pengendalian secara capaian jauh (*remote*) atau *onsite*. Sekiranya laporan tersebut memerlukan bantuan pihak NACSA, permohonan akan dihantar bagi mendapatkan maklum balas pihak NACSA.

Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan akan dihantar melalui pihak NACSA dan khidmat nasihat akan disalurkan. MARACERT seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya Pelan Pengurusan Kesinambungan Perkhidmatan/ *Business Continuity Management* (BCM) perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CIO bagi mengaktifkan Pelan BCM.

Laporan insiden yang tidak memerlukan Pelan BCM akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan. Carta lengkap mengenai perjalanan laporan insiden adalah seperti di Lampiran 3.

PKSMARA - 0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif:

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

PKSMARA - 060201 Perkhidmatan Penyampaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Semua Pengguna

a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;

b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa;

c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko; dan

d) Pembekal perlu menandatangani perakuan Akta Rahsia Rasmi seperti di Lampiran 2 untuk menjamin kerahsiaan maklumat MARA.

PKSMARA - 0603 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

PKSMARA - 060301 Perancangan Kapasiti

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. — Pentadbir Sistem ICT dan ICTSO

Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

PKSMARA - 060302 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Pengujian tersebut perlu dilaksanakan dan didokumenkan mengikut kesesuaian untuk rujukan dari semasa ke semasa. — Pentadbir Sistem ICT dan ICTSO

PKSMARA - 0604 Perisian Berbahaya

Objektif:

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti *virus, trojan* dan sebagainya.

PKSMARA - 060401 Perlindungan dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Semua Pengguna, ICTSO dan Pentadbir Sistem ICT

a) 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;

b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;

c) Mengimbas semua perisian atau sistem dengan *antivirus* sebelum menggunakannya;

d) Mengemaskini *antivirus* dengan *pattern antivirus* yang terkini;

e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan;

i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan *virus*; dan

j) Memastikan setiap pemasangan perisian yang bukan standard MARA telah mendapat kelulusan ICTSO dengan sokongan Pengawal Pusat dan direkodkan.

PKSMARA - 060402 Perlindungan dari *Mobile Code*

Penggunaan *mobile code* terutamanya dari Internet dan e-mel seperti *JavaScript, VBScript* dan *ActiveX Controls*, yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan. — Semua Pengguna

PKSMARA - 0605 *Housekeeping*

Objektif:

Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

PKSMARA - 060501 *Backup*

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan secara berkala dan setiap kali konfigurasi berubah. — Semua Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;

b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat;

c) 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;

d) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan

e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.

PKSMARA - 0606 Pengurusan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

PKSMARA - 060601 Kawalan Infrastruktur Rangkaian

Semua Pengguna, dan Pentadbir Sistem ICT

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;

b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;

c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;

d) Semua peralatan mestilah melalui proses *User Acceptance Test (UAT)* semasa pemasangan dan konfigurasi;

e) *Firewall* dipasang, dikonfigurasi dan diselenggarakan oleh pembekal dan hendaklah dipantau oleh Pentadbir Sistem ICT;

f) Semua perkakasan rangkaian yang dibekalkan oleh MAMPU (contoh: *BMT/Router*) tidak dibenarkan dialih dan dipinda konfigurasinya tanpa kebenaran ICTSO;

g) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MARA;

h) Memasang perisian *Intrusion Prevention System (IPS)* bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MARA;

i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MARA adalah tidak dibenarkan;

k) Semua pengguna hanya dibenarkan menggunakan rangkaian MARA. Penggunaan modem/ *Wireless Broadband* adalah dilarang sama sekali kecuali mendapat kebenaran ICTSO;

l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.

m) Perkhidmatan *wireless* untuk kegunaan awam hendaklah diasingkan daripada rangkaian dalaman MARA;

n) Sebarang perkakasan yang disambungkan ke rangkaian MARA adalah tidak dibenarkan membuat capaian menggunakan *bypass proxy* dan *Virtual Private Network (VPN)* yang tidak dibenarkan atau yang seumpama dengannya;

o) Penggunaan VPN bagi capaian aplikasi dalaman MARA perlu mendapatkan kelulusan ICTSO dan sokongan Pengawal Pusat.

p) Konfigurasi semua perkakasan rangkaian dan keselamatan ICT hendaklah sentiasa dikemas kini berdasarkan keperluan semasa. Salinan konfigurasi hendaklah disimpan oleh Pentadbir Sistem Keselamatan ICT pada storan pendua sebagai *backup*; dan

q) Konfigurasi rangkaian daripada LAN ke WAN perlu *transparent* (tanpa NAT) seperti alamat IP yang dibekalkan oleh pihak pembekal WAN kecuali segmen untuk *Wi-Fi*.

PKSMARA - 0607 Pengurusan Media

Objektif:

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

PKSMARA - 060701 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu dengan menandatangani perakuan Akta Rahsia Rasmi seperti di **Lampiran 2.** Penghantaran atau pemindahan media yang mengandungi maklumat terperingkat ke luar pejabat hendaklah mendapatkan kebenaran daripada CIO terlebih dahulu. — Semua Pengguna

a) Melabelkan semua media elektronik mengikut ketetapan pemeringkatan berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017);

b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;

c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja. Pengedaran kepada pihak luar hendaklah disertakan bersama perakuan Akta Rahsia Rasmi seperti di **Lampiran 2**;

d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;

e) Menyimpan semua media di tempat yang selamat; dan

f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat. Rujukan kepada Garis Panduan Sanitasi Data Sektor Awam hendaklah dibuat.

PKSMARA - 060702 Prosedur Pengendalian Media

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: — Semua Pengguna

a) Melabelkan semua media elektronik mengikut ketetapan pemeringkatan berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017);

b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;

c) Memastikan pengeluaran data atau media selepas mendapatkan kebenaran CIO serta mendatangani perakuan Akta Rahsia Rasmi seperti di **Lampiran 2**;

d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;

e) Menyimpan semua media di tempat yang selamat; dan

f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat. Rujukan kepada Garis Panduan Sanitasi Data Sektor Awam hendaklah dibuat.

PKSMARA - 060703 Keselamatan Sistem Dokumentasi

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: — Semua Pengguna

a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;

b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan

c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.

PKSMARA - 0608 Pengurusan Pertukaran Maklumat

Objektif:

Memastikan keselamatan pertukaran maklumat dan perisian antara MARA dan agensi luar terjamin.

PKSMARA - 060801 Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Semua Pengguna

a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;

b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MARA dengan agensi luar;

c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MARA; dan

d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.

PKSMARA - 060802 Pengurusan Mel Elektronik (E-mel)

Penggunaan e-mel di MARA hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam pekeliling yang dikeluarkan oleh MARA iaitu Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk *"Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"* dan mana-mana undang-undang bertulis yang berkuat kuasa.

Semua Pengguna

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:

a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MARA sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

b) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi, dan pastikan alamat e-mel penerima adalah betul;

c) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi;

d) Pengguna dinasihatkan menggunakan fail kepilan sekiranya perlu. Kaedah pemampatan (*compress*) untuk mengurangkan saiz adalah disarankan;

e) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui. Jika terdapat sebarang keraguan perlu dilaporkan kepada Pentadbir e-mel pada kadar segera;

f) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

g) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

h) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

i) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing;

j) Sebarang pertukaran status pengguna (bertukar gelaran, bertukar pusat, bersara, diberhentikan, tidak dapat dikesan, meninggal dunia dan sebagainya) perlu dimaklumkan kepada Pentadbir E-mel oleh Pengawal Pusat bagi tujuan pengemaskinian rekod e-mel;

k) E-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang bersesuaian; dan

l) Menggunakan kaedah enkripsi (*encryption*) bagi dokumen terperingkat yang dihantar secara elektronik bagi pematuhan kepada perenggan 134 Arahan Keselamatan (Semakan dan Pindaan 2017).

PKSMARA - 0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)

Objektif:

Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

PKSMARA - 060901 E-Dagang

Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. — Semua Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;

b) Maklumat yang terlibat dalam transaksi dalam talian *(online)* perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan

c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

PKSMARA - 060902 Maklumat Umum

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: — Semua Pengguna

a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;

b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan

c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.

PKSMARA - 0610 Pemantauan

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

PKSMARA - 061001 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: ICTSO

a) Sebarang percubaan pencerobohan kepada sistem ICT MARA;

b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);

c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;

d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;

e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;

f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian;

g) Aktiviti penyalahgunaan akaun e-mel; dan

h) Aktiviti penukaran alamat IP (*IP address*) dan segmen IP selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.

PKSMARA - 061002 Jejak Audit

Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara (*event*). Pentadbir Sistem ICT

Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

a) Rekod setiap aktiviti transaksi;

b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;

c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan

d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat (Akta Aktiviti Kerajaan Elektronik 2007) dan Akta Arkib Negara.

Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

PKSMARA - 061003 Sistem Log

Pentadbir Sistem ICT

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera;

c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO; dan

d) 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 server;

   ii. Fail log servis (contoh: *web, e-mel*);

   iii. Fail log aplikasi (*audit trail*); dan

   iv. Fail log rangkaian (contoh : *core switch, firewall,* IPS)

PKSMARA - 061004 Pemantauan Log

Pentadbir Sistem ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;

b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala;

c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;

d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;

e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan

f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MARA atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

BIDANG 07: KAWALAN CAPAIAN

PKSMARA - 0701 Dasar Kawalan Capaian
PKSMARA - 070101 Keperluan Kawalan Capaian

PKSMARA - 0702 Pengurusan Capaian Pengguna
PKSMARA - 070201 Akaun Pengguna
PKSMARA - 070202 Hak Capaian
PKSMARA - 070203 Pengurusan Kata Laluan
PKSMARA - 070204 *Clear Desk* dan *Clear Screen*

PKSMARA - 0703 Kawalan Capaian Rangkaian
PKSMARA - 070301 Capaian Rangkaian
PKSMARA - 070302 Capaian Internet

PKSMARA - 0704 Kawalan Capaian Sistem Pengoperasian
PKSMARA - 070401 Capaian Sistem Pengoperasian

PKSMARA - 0705 Kawalan Capaian Aplikasi dan Maklumat
PKSMARA - 070501 Capaian Aplikasi dan Maklumat

PKSMARA - 0706 Peralatan Mudah Alih dan Kerja Jarak Jauh
PKSMARA - 070601 Peralatan Mudah Alih
PKSMARA - 070602 Kerja Jarak Jauh
PKSMARA - 070603 *Bring Your Own Device (BYOD)*

BIDANG 07:

KAWALAN CAPAIAN

PKSMARA - 0701 Dasar Kawalan Capaian

Objektif:
Mengawal capaian ke atas maklumat.

PKSMARA - 070101 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.

Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;

b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;

c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan

d) Kawalan ke atas kemudahan pemprosesan maklumat.

PKSMARA - 0702 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT MARA.

PKSMARA - 070201 Akaun Pengguna

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.

Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:

Semua Pengguna, Pentadbir Sistem ICT dan ICTSO

a) Akaun yang diperuntukkan oleh MARA sahaja boleh digunakan;

b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;

c) Akaun pengguna yang diwujudkan akan diberi tahap capaian mengikut keperluan dan hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;

d) Permohonan akaun pengguna bagi staf dari subsidiari MARA, pembekal, pelajar praktikal atau lain-lain yang bukan kakitangan MARA perlu mendapat kelulusan ICTSO terlebih dahulu;

e) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MARA. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;

f) Pentadbir Sistem ICT boleh menamatkan akaun pengguna atas sebab-sebab berikut:

i. Bertukar ke agensi lain;

ii. Bersara;

iii. Menamatkan perkhidmatan; atau

iv. Ditamatkan perkhidmatan.

g) Bagi akaun pengguna yang tidak aktif, pentadbir sistem perlu menyemak status semasa pengguna sebelum sebarang tindakan yang bersesuaian diambil. Semakan ID tidak aktif perlu dilakukan sekurang-kurangnya empat (4) kali setahun.

PKSMARA - 070202 Hak Capaian

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.

Pentadbir Sistem ICT

PKSMARA - 070203 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MARA seperti berikut:

a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka atau aksara khusus;

d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun. Penyimpanan kata laluan secara automatik sama ada pada *browser* atau sebarang perisian pihak ketiga adalah tidak dibenarkan.

e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

Semua Pengguna dan Pentadbir Sistem ICT

f) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;

g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;

h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

i) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian;

j) Mengelakkan penggunaan semula kata laluan yang baru digunakan.

k) Pengguna dilarang menggunakan sebarang maklumat peribadi sebagai kata laluan;

l) Sistem aplikasi yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna;

m) Sebarang urusan pertukaran kata laluan melalui telefon dan e-mel perlu mengambil langkah-langkah keselamatan yang bersesuaian; dan

n) Pentadbir sistem ICT di semua pusat perlu bertanggungjawab ke atas akaun *administrator* dan kata laluan untuk semua perkakasan ICT di pusat masing-masing.

PKSMARA - 070204 *Clear Desk* dan *Clear Screen*

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. — Semua Pengguna

Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;

b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan

c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

PKSMARA - 0703 Kawalan Capaian Rangkaian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

PKSMARA - 070301 Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: — Pentadbir Sistem ICT dan ICTSO

a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MARA, rangkaian agensi lain dan rangkaian awam;

b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;

c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;

d) Mengawal capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi; dan

e) Menyediakan polisi bagi mengawal capaian bagi semua rangkaian yang dikongsi *(shared networks)*, terutama sekali yang keluar daripada rangkaian MARA.

PKSMARA - 070302 Capaian Internet

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Pengurus ICT, Pentadbir Sistem ICT, ICTSO dan Semua Pengguna

a) Penggunaan Internet di MARA hendaklah dipantau secara berterusan 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 MARA;

b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;

c) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

d) Pentadbir Sistem ICT berhak untuk memantau penggunaan Internet bagi pengguna yang menggunakan sistem rangkaian MARA atau perkakasan ICT yang disediakan oleh MARA;

e) Penggunaan teknologi *Bandwitdh Management System* untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;

f) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/ pegawai yang diberi kuasa;

g) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

h) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian berkenaan sebelum dimuat naik ke Internet;

i) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

j) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MARA;

k) Pengguna MARA dilarang daripada memuat naik sebarang dokumen rasmi, perisian berlesen, e-mel dan sebagainya ke *server* atau ruang storan yang dipunyai oleh pihak luar tanpa sebarang kebenaran daripada ICTSO;

l) Pengguna MARA yang menggunakan akaun MARA (mara.gov.my) merupakan wakil MARA. Oleh itu, setiap kakitangan diingatkan supaya tidak menggunakan akaun tersebut untuk tujuan komersial, politik, perjudian, jenayah dan melanggan sebarang perkhidmatan *online*;

m) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam dan media sosial. Walau bagaimanapun, kandungan perbincangan awam ini tertakluk kepada dasar dan peraturan yang telah ditetapkan;

n) Internet tidak menjamin kerahsiaan maklumat. Maklumat sensitif yang dihantar melalui Internet terdedah kepada risiko dikesan oleh pihak ketiga. Semua pengguna perlu berhati-hati dan berwaspada apabila menghantar sebarang maklumat melalui Internet;

o) Penggunaan sebarang bentuk modem persendirian untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali;

p) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:

i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet.

ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

iii. Menggunakan perkhidmatan *proxy* atau VPN bagi tujuan *bypass* sistem rangkaian MARA bagi tujuan capaian Internet.

q) Setiap pengguna MARA bertanggungjawab ke atas sebarang salah perlakuan dan tindakan yang diambil sewaktu menggunakan kemudahan Internet yang diberikan; dan

r) ICTSO atau wakil yang dibenarkan ICTSO berhak untuk memeriksa setiap komputer yang yang dibekalkan oleh MARA atau menggunakan rangkaian komputer MARA untuk memastikan setiap arahan di dalam pelan ini dipatuhi oleh semua kakitangan.

PKSMARA - 0704 Kawalan Capaian Sistem Pengoperasian

Objektif:

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

PKSMARA - 070401 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer.

Pentadbir Sistem ICT dan ICTSO

Kemudahan ini juga perlu bagi:

a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan

b) Merekodkan capaian yang berjaya dan gagal.

Kaedah-kaedah yang digunakan hendaklah menyokong perkara-perkara berikut:

a) Mengesahkan pengguna yang dibenarkan;

b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *administrator*; dan

c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;

b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;

c) Mengehadkan dan mengawal penggunaan program;

d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi; dan

e) Memastikan sistem pengurusan kata laluan yang interaktif dan memastikan kata laluan adalah berkualiti.

PKSMARA - 0705 Kawalan Capaian Aplikasi dan Maklumat

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.

PKSMARA - 070501 Capaian Aplikasi dan Maklumat

Pentadbir Sistem ICT dan ICTSO

Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:

a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;

b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem *log/audit trail*);

c) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah;

d) Capaian sistem maklumat dan aplikasi melalui jarak jauh hanya dibenarkan mengikut keperluan dan penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja;

e) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;

f) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;

g) Memastikan maklumat tarikh *login* terakhir dipamerkan; dan

h) Memastikan *session timeout* dilaksanakan.

PKSMARA - 0706 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif:

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

PKSMARA - 070601 Peralatan Mudah Alih

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Peralatan mudah alih yang dibekalkan oleh MARA seperti telefon pintar, *tablets* dan yang seumpamanya hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; — Semua Pengguna

b) Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih;

c) Ketika menggunakan rangkaian komputer awam (*public Wi-Fi*), capaian kepada dokumen berperingkat hendaklah dihadkan. Sekiranya masih ada keperluan untuk berbuat demikian, maka langkah-langkah keselamatan hendaklah diambil supaya maklumat tersebut tidak boleh dilihat oleh pihak yang tidak berkenaan;

d) Peralatan mudah alih hendaklah dilengkapkan dengan sistem pengoperasian dan perisian *antivirus* yang telah diselenggarakan dan sentiasa dikemaskini dengan baik;

e) Maklumat dokumen berperingkat tidak dibenarkan untuk disimpan di dalam peralatan mudah alih tanpa kebenaran CIO; dan

f) Proses *backup* perlu dilaksanakan bagi menjamin keselamatan data

PKSMARA - 070602 Kerja Jarak Jauh

Perkara yang perlu dipatuhi adalah seperti berikut: — Pengurus ICT, Pentadbir Sistem ICT, ICTSO dan Semua Pengguna

a) Capaian jarak jauh yang dimaksudkan merangkumi capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *telecommuting*;

b) Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (*encryption*);

c) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan;

d) Lokasi bagi akses ke sistem ICT MARA hendaklah dipastikan selamat;

e) Penggunaan perkhidmatan menggunakan kaedah VPN yang disediakan oleh MARA hendaklah mendapat kebenaran daripada Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; dan

f) Kebenaran bagi capaian jarak jauh oleh pihak pembekal perlu diteliti semula terutama yang melibatkan sistem-sistem kritikal. Perlu ada seliaan/pemantauan khas dari pihak MARA apabila pembekal membuat capaian jarak jauh.Ia perlu mengambilkira lokasi asal capaian dan risiko-risiko serta ancaman kepada pihak MARA.

PKSMARA - 070603 ***Bring Your Own Device (BYOD)***

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Pengguna MARA perlu memastikan keselamatan maklumat semasa menggunakan peralatan BYOD; — Semua Pengguna

b) Pengguna BYOD adalah dilarang memasang perisian yang tidak dibenarkan untuk melaksanakan tugasan rasmi MARA;

c) Pengguna BYOD adalah dilarang memasang perisian yang mengganggu sistem rangkaian MARA;

d) Mengaktifkan fungsi keselamatan kata laluan di setiap komputer riba/peranti. Sekiranya *Active Directory* wujud, komputer berkenaan perlu sambung ke *Domain Server*;

e) Perkakasan BYOD hendaklah dilindungi oleh perisian *antivirus* bagi mengelak penyebaran virus/ *malware/trojan* dan lain-lain ke atas pengguna MARA yang lain;

f) Pengguna BYOD perlu memastikan peranti yang digunakan menggunakan teknologi enkripsi (*encryption*), tandatangan digital atau sebarang mekanisme bagi melindungi maklumat elektronik semasa ianya digunakan;

g) Pengguna BYOD adalah dilarang menyalin dan membawa keluar maklumat MARA dengan menggunakan peranti mudah alih dan media storan seperti *USB, external hardisk* dan sebagainya;

h) Pengguna BYOD perlu memadam dokumen elektronik dengan memadam secara elektronik/ *secure deletion* selepas dokumen tidak lagi diguna pakai;

i) Pengguna BYOD adalah dilarang meninggalkan komputer riba/peranti di ruang pejabat yang terbuka tanpa menguncikannya dengan kabel keselamatan; dan

j) Perkakasan BYOD yang membuat sambungan ke rangkaian MARA adalah tidak dibenarkan membuat capaian menggunakan *proxy* luar, VPN yang tidak dibenarkan atau yang seumpama dengannya.

BIDANG 08: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

PKSMARA - 0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

PKSMARA - 080101 Keperluan Keselamatan Sistem Maklumat

PKSMARA - 080102 Pengesahan *Data Input* dan *Output*

PKSMARA - 0802 Kawalan Kriptografi

PKSMARA - 080201 Enkripsi Dan Pengurusan Infrastruktur Kunci Awam (PKI)

PKSMARA - 0803 Keselamatan Fail Sistem

PKSMARA - 080301 Kawalan Fail Sistem

PKSMARA - 0804 Keselamatan Dalam Proses Pembangunan dan Sokongan

PKSMARA - 080401 Prosedur Kawalan Perubahan

PKSMARA - 080402 Pembangunan Perisian Secara *Outsource*

PKSMARA - 0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)

PKSMARA - 080501 Kawalan dari Ancaman Teknikal

BIDANG 08:

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

PKSMARA - 0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:
Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

PKSMARA - 080101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Pemilik Sistem, Pentadbir Sistem ICT dan Pentadbir Sistem ICT dan Pentadbir Sistem ICT dan Pentadbir Sistem ICT dan ICTSO

a) Setiap pembangunan sistem baru, penyelenggaraan sistem dan peningkatan sistem perlu mengambilkira ciri-ciri keselamatan dan diperakui oleh Ahli Jawatankuasa ICT dimana ICTSO adalah sebahagian dari Jawatankuasa tersebut;

b) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;

c) 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;

d) Ujian keselamatan perlu dijalankan ke atas sistem yang berisiko tinggi berdasarkan standard industri semasa (Contoh : OWASP);

e) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan;

f) 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;

g) Pembangunan sistem baharu yang menggunakan perkhidmatan *hosting* di *public cloud* perlu mendapatkan kebenaran ICTSO; dan

h) Pelaksanaan sistem berhubung dengan kelengkapan, bahan serta maklumat rasmi yang mempunyai ciri-ciri keselamatan menggunakan aplikasi berteknologi tinggi dan terkini termasuk sistem ICT hendaklah terlebih dahulu dirujuk dan mendapatkan pandangan daripada Ketua Pengarah Keselamatan Kerajaan bagi tujuan penilaian risiko keselamatan. Pembekal perkhidmatan yang membangunkan sistem-sistem tertentu bagi pihak MARA hendaklah menyerahkan segala maklumat, bahan yang berkaitan serta kod sumber (*source code*) dan seumpamanya menjadi milik MARA sepenuhnya. Bagi meningkatkan tahap keselamatan ICT, peranti, perkakasan, perisian, aplikasi, sistem ICT dan sebagainya yang telah mendapat pensijilan keselamatan ICT dan diiktiraf oleh Kerajaan boleh dipertimbangkan.

PKSMARA - 080102 Pengesahan *Data Input* dan *Output*

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Pemilik Sistemdan Pentadbir Sistem ICT

a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan

b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

PKSMARA - 0802 Kawalan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

PKSMARA - 080201 Enkripsi Dan Pengurusan Infrastruktur Kunci Awam (PKI)

Melindungi kerahsiaan, integriti dan kesahihan maklumat yang merangkumi data di dalam sistem rangkaian, sistem aplikasi dan pangkalan data. Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. — Semua Pengguna

Kriptografi turut merangkumi kaedah-kaedah seperti berikut:

a) Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*);

b) Tandatangan Digital Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan; dan

c) Pengurusan Infrastruktur Kunci Awam atau *Public Key Infrastructure (PKI)* Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

Rujukan berkaitan kriptografi seperti Dasar Kriptografi Negara dan MySeal yang dikeluarkan oleh Cybersecurity Malaysia boleh digunapakai sebagai panduan.

PKSMARA - 0803 Keselamatan Fail Sistem

Objektif:

Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

PKSMARA - 080301 Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; — Semua Pengguna

b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;

c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;

d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan

e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

PKSMARA - 0804 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

PKSMARA - 080401 Prosedur Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambah baikan dan pembetulan yang dilakukan oleh pembekal; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan; e) Menghalang sebarang peluang untuk membocorkan maklumat; dan f) Sebarang perubahan perlu direkodkan menggunakan Borang *Change Request* seperti yang ditetapkan.	Pemilik Sistem dan Pentadbir Sistem ICT

PKSMARA - 080402 Pembangunan Perisian Secara *Outsource*

Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kerja-kerja pembangunan perisian perlu dilakukan di premis MARA atau lokasi yang dibenarkan oleh ICTSO sahaja. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik MARA.	Pentadbir Sistem ICT dan ICTSO

PKSMARA - 0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Objektif:

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

PKSMARA - 080501 Kawalan dari Ancaman Teknikal

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; — Pentadbir Sistem ICT

b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan

c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

BIDANG 09: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

PKSMARA - 0901 Mekanisme Pelaporan Insiden Keselamatan ICT

PKSMARA - 090101 Mekanisme Pelaporan
PKSMARA - 090102 Mekanisme Pelaporan Insiden Bukan ICT

PKSMARA - 0902 Pengurusan Maklumat Insiden Keselamatan ICT

PKSMARA - 090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

BIDANG 09:

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

PKSMARA - 0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:
Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

PKSMARA - 090101 Mekanisme Pelaporan

MARACERT, Pentadbir Sistem ICT, ICTSO

Pusat Kawalan dan Koordinasi Siber Negara (NC4) menyediakan platform bagi perkongsian maklumat berkaitan insiden siber untuk seluruh Prasarana Maklumat Kritikal Negara (CNII).

CNII merujuk kepada aset (fizikal dan maya), sistem dan fungsi yang penting kepada negara dan kepincangan terhadap fungsi-fungsi kritikal ini akan memberikan impak yang besar kepada pertahanan dan keselamatan negara, kekuatan ekonomi negara, imej negara, kemampuan kerajaan untuk berfungsi, kesihatan dan keselamatan orang awam.

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Pelan Keselamatan Siber sama ada yang ditetapkan secara tersurat atau tersirat.

a) Pelaporan semua insiden keselamatan ICT dimajukan kepada ICTSO dan MARACERT untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan;

b) MARACERT akan bertindak dan menghubungi pasukan CERT dari Kementerian yang bertanggungjawab atau NACSA sebagai makluman atau bagi mendapatkan bantuan;

c) Semua pengguna perlu segera melaporkan sebarang kejadian insiden keselamatan ICT bagi mengelakkan kerosakan bahan bukti tanpa melaksanakan tindakan secara sendirian;

d) Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak;

e) ICTSO melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT sekiranya perlu; dan

f) Pentadbir sistem yang terlibat perlu melaporkan sebarang kejadian yang melibatkan keselamatan ICT kepada MARA CERT dan ICTSO MARA.

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada Pengurus ICT, ICTSO dan NACSA 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 mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;

d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.

Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di MARA sepertimana **Lampiran 3.**

Prosedur pelaporan insiden keselamatan ICT berdasarkan Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

PKSMARA - 090102 Mekanisme Pelaporan Insiden Bukan ICT

Semua pengguna yang terlibat haruslah melaporkan dan merekod sebarang kejadian/kerosakan peralatan bukan ICT kepada pihak pentadbiran yang bertanggungjawab. — Semua Pengguna

PKSMARA - 0902 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

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

PKSMARA - 090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

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. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MARA. — ICTSO

Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan diselenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:

a) Mengenal pasti semua jenis insiden keselamatan ICT;

b) Mematuhi Pelan Pemulihan Bencana (DRP) seperti yang telah digariskan dalam Pelan Kesinambungan Perkhidmatan/*Business Continuity Management (BCM)*;

c) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;

d) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;

e) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;

f) Menyediakan tindakan pemulihan segera; dan

g) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

BIDANG 10: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

PKSMARA - 1001 Dasar Kesinambungan Perkhidmatan

PKSMARA - 100101 Pelan Kesinambungan Perkhidmatan

PKSMARA - 100102 Pelan Pemulihan Bencana

BIDANG 10:

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

PKSMARA - 1001 Dasar Kesinambungan Perkhidmatan

Objektif:
Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

PKSMARA - 100101 Pelan Kesinambungan Perkhidmatan

Pengurusan Kesinambungan Perkhidmatan (*Business Continuity Management*) adalah mekanisme bagi mengurus dan memastikan kepentingan pemegang taruh sistem penyampaian perkhidmatan dilindungi dan imej MARA terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan MARA di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan.

Bahagian Pengurusan Risiko dan Inspektorat, Pengurus CIO dan ICTSO

Ketua Pegawai Maklumat (CIO) adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT MARA.

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

b) Senarai pengguna berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan pegawai yang tidak dapat hadir untuk menangani insiden;

c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;

d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan.

Salinan Pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian Pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

MARA hendaklah memastikan salinan Pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

PKSMARA - 100102 Pelan Pemulihan Bencana

Pelan Pemulihan Bencana (DRP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKICT MARA dan perkara-perkara berikut perlu diberi perhatian:	CIO, ICTSO dan Pengurus ICT

a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan dan pemulihan;

b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;

c) Mendokumentasikan proses dan prosedur yang telah dipersetujui;

d) Mengenalpasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;

e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;

f) Membuat *backup*; dan

g) Menguji dan mengemas kini pelan sekurang-kurangnya tiga tahun sekali.

BIDANG 11: PEMATUHAN

PKSMARA - 1101 Pematuhan dan Keperluan Perundangan

PKSMARA - 110101 Pematuhan Dasar
PKSMARA - 110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal
PKSMARA - 110103 Pematuhan Keperluan Audit
PKSMARA - 110104 Keperluan Perundangan
PKSMARA - 110105 Pelanggaran Dasar

BIDANG 11:

PEMATUHAN

PKSMARA - 1101 Pematuhan dan Keperluan Perundangan

Objektif:
Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Pelan Keselamatan Siber MARA.

PKSMARA - 110101 Pematuhan Pelan

Setiap pengguna di MARA hendaklah membaca, memahami dan mematuhi Pelan Keselamatan Siber MARA dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. — Semua Pengguna MARA

Semua aset ICT di MARA termasuk maklumat yang disimpan di dalamnya adalah hak milik MARA. Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

Sebarang penggunaan aset ICT MARA selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MARA.

PKSMARA - 110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. — ICTSO

Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.

Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment (SPA)* mestilah dijalankan oleh individu yang kompeten dan dibenarkan.

PKSMARA - 110103 Pematuhan Keperluan Audit

Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan. — Semua Pengguna MARA

Audit Dalam

Semakan audit dalam adalah perlu bagi memastikan pematuhan terhadap peraturan dan polisi yang berkuat kuasa. Pasukan audit dalam yang terlatih hendaklah ditubuhkan bagi melaksanakan audit dalam. Audit Pematuhan ICT yang dikendalikan oleh Pasukan Audit yang dilantik hendaklah dilaksanakan setiap tahun. Skop pematuhan ICT hendaklah meliputi pematuhan terhadap Pelan Keselamatan Siber MARA.

Audit Luar

Semakan audit luar adalah perlu bagi memastikan pematuhan kepada peraturan dan polisi yang sedang berkuat kuasa dan hasil semakan semula audit dalam. Audit luar hendaklah dilaksanakan oleh pihak yang tiada kepentingan terhadap Jabatan dan sistem yang diaudit. Juruaudit Luar yang dilantik mestilah mempunyai persijilan yang diiktiraf oleh kerajaan Malaysia.

Pensijilan khas audit luar seperti ISMS, Pengurusan Kesinambungan Perkhidmatan dan *Common Criteria,* hendaklah dilaksanakan oleh badan yang diiktiraf oleh Kerajaan.

PKSMARA - 110104 Keperluan Perundangan

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MARA:

Semua Pengguna MARA

i. Arahan Keselamatan (Semakan dan Pindaan 2017);

ii. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

iii. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002;

iv. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

v. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;

vi. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

vii. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

viii. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar *(Wireless Local Area Network)* di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;

ix. Surat Arahan Ketua Pengarah MARA - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

x. Surat Arahan Ketua Pengarah MARA - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

xi. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

xii. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

xiii. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

xiv. Akta Tandatangan Digital 1997;

xv. Akta Rahsia Rasmi 1972;

xvi. Akta Jenayah Komputer 1997;

xvii. Akta Hak Cipta (Pindaan) Tahun 2012;

xviii. Akta Komunikasi dan Multimedia 1998;

xix. Perintah-Perintah Am;

xx. Arahan Perbendaharaan;

xxi. Arahan Teknologi Maklumat 2007;

xxii. Garis Panduan Pengurusan Keselamatan Perlindungan 2015.

xxiii. Surat Pekeliling Am MARA Bilangan 2 Tahun 2018: Pelaksanaan Pengurusan Risiko MARA;

xxiv. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA)

xxv. Surat Edaran Unit Penyelaras Bil. 9/2018: Pindaan Keahlian, Kuasa dan Bidang Tugas bagi Jawatankuasa Pemandu ICT (JPICT) MARA.

xxvi. Surat Arahan Ketua Setiausaha Negara- Penamaan Ketua Pegawai Maklumat Sektor Awam bertarik 22 Mac 2000.

xxvii. Lampiran C Pekeliling Perkhidmatan Bilangan 15 Tahun 2006.

xxviii. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan Ms ISO/IEC 27001:2007 Dalam Sektor Awam.

xxix. Pemantapan Penggunaan Dan Pengurusan E-Mel Di Agensi-Agensi Kerajaan Bertarikh 1 Julai 2010.

xxx. Surat Arahan Ketua Pengarah - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam Bertarikh 24 November 2010.

xxxi. Surat Pekeliling Am MARA Bil. 2/2015 Tatacara Pengurusan Aset Alih MARA.

xxxii. Manual Pengurusan Keselamatan Perlindungan Mara Edisi 2.

xxxiii. Garis Panduan Pengurusan Pusat Data MAMPU.

xxxiv. Garis Panduan Sanitasi Media Elektronik Sektor Awam 2018.

xxxv. Akta Aktiviti Kerajaan Elektronik 2007.

xxxvi. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT. (ICTSO) Sektor Awam oleh NACSA bertarikh 28 Februari 2019.

xxxvii. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team* (GCERT) oleh NACSA bertarikh 28 Januari 2019.

xxxviii. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Risiko Keselamatan Maklumat Menggunakan MyRAM App 2.0 di Agensi Sektor Awam.

xxxix. Surat Arahan Ketua Pengarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam bertarikh 22 Jan 2010.

xl. Surat Arahan Ketua Pengarah MAMPU - Pengaktifan *Fail Log Server* Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-Agensi Kerajaan bertarikh 23 Mac 2009.

xli. Surat Edaran Bahagian Pengurusan Risiko Dan Inspektorat MARA Bil.2-2018 Pelaksanaan Tapisan Keselamatan dan Pemusatan Pegawai Pengesah e-VETTING di Majlis Amanah Rakyat bertarikh 7 Mei 2018.

xlii. Surat Edaran Bahagian Pemantauan dan Inspektorat MARA Bil. 11-2015 Manual Garis Panduan Pengurusan Keselamatan Perlindungan bertarikh 30 Disember 2015.

PKSMARA - 110105 Pelanggaran Pelan

Pelanggaran Pelan Keselamatan Siber MARA boleh dikenakan tindakan tatatertib.	Semua Pengguna MARA

GLOSARI

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, cakera keras, pita magnetik, *optical disk, flash disk, thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses salinan 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.
Browser	Pelayar atau penjelajah media
BYOD	*Bring Your Own Device* Merujuk kepada pekerja yang membawa peranti pengkomputeran mereka sendiri - seperti telefon pintar, komputer riba dan tablet PC - untuk bekerja dengan mereka dan menggunakannya sebagai tambahan kepada atau bukan peranti yang disediakan oleh majikan.
Bypass proxy	Capaian Internet atau rangkaian dengan menggunakan perkhidmatan *proxy server* dari pihak ketiga bagi tujuan pemintasan.
CCTV	*Closed-Circuit television* Kamera video digital yang berfungsi untuk memantau dan menghantar signal video pada suatu ruang simpanan yang kemudian signal itu akan dipancarkan ke layar monitor.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Common Criteria	Merupakan metodologi penilaian keselamatan yang dibangunkan untuk menentukan dan membantu pelaksanaan penilaian yang konsisten mengenai produk dan sistem keselamatan. Ia menggalakkan pengiktirafan antarabangsa dan kepercayaan dari global terhadap kualiti produk dan sistem keselamatan.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.

Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage),* penipuan *(hoaxes*).
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu port kepada semua *port* yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Login	*Log-In* komputer Masuk ke dalam sesuatu sistem atau aplikasi komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus, Trojan horse, worm, spyware* dan sebagainya.
MERT	*MARA Emergency Response Team*

MODEM	*MOdulator DEModulator* Peranti yang boleh menukar isyarat digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
NACSA	*The National Cyber Security Agency (NACSA)* atau Agensi Keselamatan Siber Negara Agensi utama negara bagi hal-hal keselamatan siber, dengan objektif untuk mengamankan dan memperkuat daya tahan Malaysia dalam menghadapi ancaman serangan siber, dengan menyelaras dan menyatukan negara terbaik pakar dan sumber dalam bidang keselamatan siber.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
OWASP	*The Open Web Application Security Project* Projek Keselamatan Aplikasi Web Terbuka adalah organisasi amal yang tidak berasaskan keuntungan yang memberi tumpuan kepada peningkatan keselamatan perisian/aplikasi web.
Pegawai Aset	Pegawai yang dilantik untuk menjaga aset di pusat MARA.
Pelanggan	Penguna awam dan pengguna MARA
Pelan BCM	Pelan *Business Continuity Management* atau Pelan Kesinambungan Perkhidmatan Proses pengurusan holistik yang mengenal pasti potensi kesan yang mengancam organisasi, dan menyediakan rangka kerja untuk membangun daya tahan dan keupayaan untuk bertindak balas yang berkesan yang melindungi kepentingan pemegang kepentingan utama, reputasi, jenama dan penciptaan nilai aktiviti.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Public Wi-fi	Wi-fi awam yang telah disediakan oleh pihak tertentu (seperti di restoran) secara percuma.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Remote Access	Kawalan jauh komputer dengan menggunakan peranti lain yang disambungkan melalui internet atau rangkaian lain.

Session Time-out	Waktu tamat sesi mewakili peristiwa yang berlaku apabila pengguna tidak melakukan apa-apa tindakan di laman web/ sistem aplikasi pada sela waktu yang ditetapkan.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Source Code	Kod Sumber Program komputer dalam bahasa pengaturcaraan asalnya (seperti FORTRAN atau C) sebelum terjemahan ke kod objek biasanya oleh pengkompil.
Storan Awan (*Cloud Storage*)	Media penyimpanan online yang membolehkan pengguna menyimpan data/ maklumat di pelayan mata *(server virtual)* yang tersedia.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection (CSMA/CD)* yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Telecommuting	Pengaturan kerja di mana pekerja bekerja di luar pejabat, sering bekerja dari rumah atau lokasi yang dekat dengan rumah (termasuk kedai kopi, perpustakaan, dan pelbagai tempat lain).
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.
Virtual Private Network (VPN)	Sambungan antara satu jaringan dengan jaringan lain secara peribadi (*private*) melalui jaringan *public* (Internet).
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
WAN	*Wide Area Network* atau Rangkaian Kawalan Luas Rangkaian yang wujud di kawasan geografi berskala besar menghubungkan rangkaian yang lebih kecil.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

SURAT AKUAN PEMATUHAN
PELAN KESELAMATAN SIBER MARA

Nama (Huruf Besar) :

No. Kad Pengenalan :

Jawatan :

Bahagian :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

Tandatangan :

Tarikh :

Pengesahan Pegawai Keselamatan ICT

Pengarah
Bahagian Teknologi Maklumat
b.p. Ketua Pengarah MARA
Tarikh:

LAMPIRAN 'D'

PERAKUAN UNTUK DITANDATANGANI OLEH PENJAWAT AWAM BERKENAAN DENGAN AKTA RAHSIA RASMI 1972

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

Saya faham bahawa segala maklumat rasmi yang saya perolehi dalam perkhidmatan Seri Paduka Baginda Yang Di Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang Di Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kerajaan.

Tandatangan : .....

Nama dengan Huruf Besar : _____

No. Kad Pengenalan : _____

Jawatan : _____

Jabatan : _____

Tarikh : _____

Disaksikan oleh : .....

(Tandatangan)

Nama dengan Huruf Besar : _____

No Kad Pengenalan : _____

Jawatan : _____

Jabatan : _____

Tarikh : _____

Cop Jabatan : .....

LAMPIRAN 'E'

PERAKUAN UNTUK DITANDATANGANI APABILA MENINGGALKAN PERKHIDMATAN KERAJAAN

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan 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 benda rahsia atau apa-apa tingkahlaku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi sesuatu kesalahan di bawah Akta tersebut yang boleh dihukum maksimum penjara seumur hidup.

Semua maklumat yang telah saya dapat atau lihat dalam masa menjalankan kewajipan-kewajipan saya adalah diliputi oleh akta tersebut. Adalah menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa maklumat itu kepada mana-mana orang lain, sama ada atau tidak orang itu memegang atau telah memegang jawatan di bawah Duli Yang Maha Mulia Seri Paduka Baginda Yang di-Pertuan Agong atau di bawah mana-mana Kerajaan Malaysia, sebelum dan selepas saya berehnti memegang jawatan itu.

Apa-apa tingkahlaku saya yang membahayakan keselamatan atau rahsia sesuatu maklumat atau apa-apa sebutan oleh saya dengan tiada kebenaran sama ada sebutan itu secara lisan atau terkandung dalam apa-apa gambarfoto, filem, negative, pita rakam, peta, pelan, model, graf, lukisan, piringhitam, runut bunyi, benda, atau lain-lain alat dsb., dan sama ada di Malaysia atau di negara luar mengenai apa-apa perkara yang telah saya ketahui atau sifat rasmi saya itu boleh menyebabkan saya didakwa di bawah Akta tersebut.

Saya mengaku abahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyaratimbal, atau katajodoh rasmi yang rahsia, atau apa-apa benda, suratan atau maklumat, anak kunci, lencana, alat meteri, atau cap bagi atau yang dipunyai atau diguna, dibuat atau diadakan oleh mana-mana Jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda yang tidak dibenarkan dalam milik atau kawalan saya.

Tandatangan : _____

Nama dengan Huruf Besar : _____

No. Kad Pengenalan : _____

Jawatan : _____

Jabatan : _____

Tarikh : _____

Disaksikan oleh : .....
(Tandatangan)

Nama dengan Huruf Besar : _____

No Kad Pengenalan : _____

Jawatan : _____

Jabatan : _____

Tarikh : _____

Cop Jabatan : .....

LAMPIRAN 'F'

PERAKUAN UNTUK DITANDATANGANI OLEH VENDOR/ KONTRAKTOR BERKENAAN DENGAN AKTA RAHSIA RASMI 1972

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

Saya faham bahawa segala maklumat rasmi yang saya perolehi dalam perkhidmatan Seri Paduka Baginda Yang Di Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang Di Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kerajaan.

Tandatangan : .....

Nama dengan Huruf Besar : _____

No. Kad Pengenalan : _____

Jawatan : _____

Jabatan : _____

Tarikh : _____

Disaksikan oleh : .....

(Tandatangan)

Nama dengan Huruf Besar : _____

No Kad Pengenalan : _____

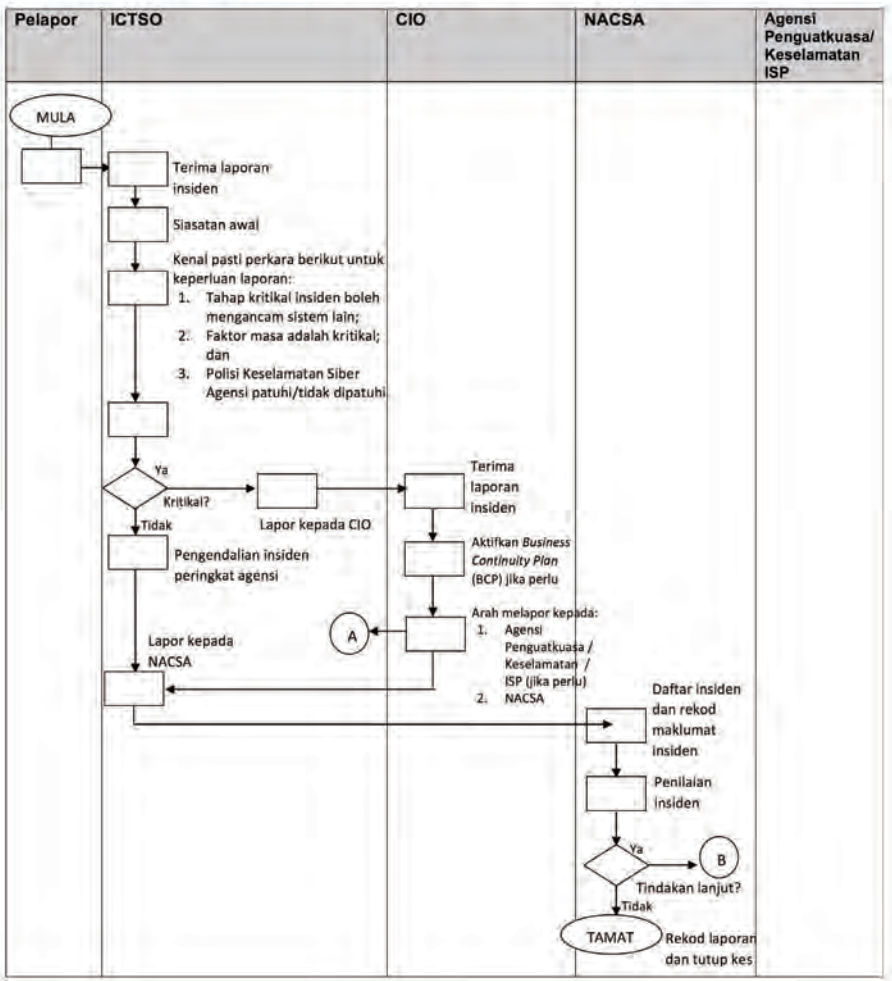
Jawatan : _____

Jabatan : _____

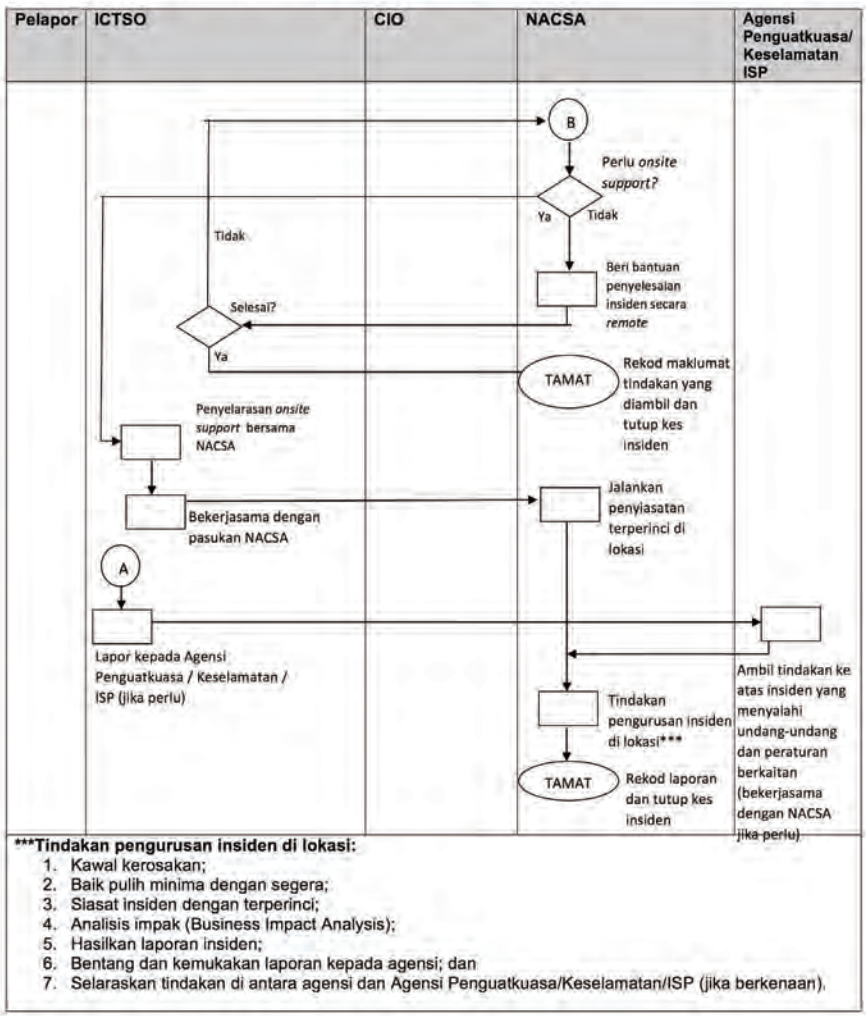
Tarikh : _____

Cop Jabatan : .....

Carta Alir Proses Kerja Pelaporan Insiden Keselamatan Siber



Carta Alir Proses Kerja Pelaporan Insiden Keselamatan Siber



***Tindakan pengurusan insiden di lokasi:**

1. Kawal kerosakan;
2. Baik pulih minima dengan segera;
3. Siasat insiden dengan terperinci;
4. Analisis impak (Business Impact Analysis);
5. Hasilkan laporan insiden;
6. Bentang dan kemukakan laporan kepada agensi; dan
7. Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/Keselamatan/ISP (jika berkenaan).

Bahagian Teknologi Maklumat MARA

www.mara.gov.my