مجلس فربندارن سلايغ
Majlis Perbandaran Selayang

DASAR KESELAMATAN ICT MAJLIS PERBANDARAN SELAYANG

Versi 3.1

MAC 2024

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
FEBRUARI 2010	1.0	Mesyuarat Pengurusan MPS	FEBRUARI 2010
24 SEPTEMBER 2013	2.0	Mesyuarat Pengurusan MPS Bil 8/2013	24 SEPTEMBER 2013
22 MAC 2018	2.1	Mesyuarat Pengurusan MPS Bil 2/2018	01 APRIL 2018
26 SEPTEMBER 2018	2.2	Mesyuarat Pengurusan MPS Bil 6/2018	01 OKTOBER 2018
29 NOVEMBER 2019	2.3	Mesyuarat Pengurusan MPS Bil 6/2019	01 DISEMBER 2019
15 OKTOBER 2021	3.0	Mesyuarat Pengurusan MPS Bil 10/2021	01 NOVEMBER 2021
19 FEBRUARI 2024	3.1	Mesyuarat Pengurusan MPS Bil 02/2024	01 MAC 2024

JADUAL PINDAAN DASAR KESELAMATAN ICT
MAJLIS PERBANDARAN SELAYANG

TARIKH	VERSI	PERKARA	PINDAAN
Februari 2024	**Versi 3.1**	**-**	1. Meminda CIO kepada CDO, Ketua Pegawai Maklumat kepada Ketua Pegawai Digital dan Chief Information Officer kepada Chief Digital Officer di keseluruhan dokumen DKICT
		050202	2. Meminda pernyataan dengan mengeluarkan perkataan disket, cakera padat, pita magnetik
		-	3. Mengosongkan nama ICTSO di Lampiran 2

ISI KANDUNGAN

PENGENALAN

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

OBJEKTIF

Dasar Keselamatan ICT MPS diwujudkan untuk menjamin kesinambungan urusan MPS dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi MPS. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT MPS ialah seperti berikut:

(a) Memastikan kelancaran operasi bahagian-bahagian dan unit dan meminimumkan kerosakan dan kemusnahan;

(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

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

PERNYATAAN DASAR

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

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

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

Dasar Keselamatan ICT MPS 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 jenis 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 MPS terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT MPS 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, Dasar Keselamatan ICT MPS 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 MPS. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan 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 MPS.

(c) Perkhidmatan

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

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

(d) Data atau Maklumat

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

(e) Manusia

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

(f) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (e) 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 Dasar Keselamatan ICT MPS 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 seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

(b) Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca 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 MPS 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 di manipulasi. 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

Dasar Keselamatan ICT MPS 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 mekanisma keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

MPS hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu MPS 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.

MPS 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 MPS 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.

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

MPS 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 DASAR

0101 DASAR KESELAMATAN ICT

Objektif:

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

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Yang DiPertua MPS dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Digital (Chief Digital Officer - CDO), Pegawai Keselamatan ICT (ICTSO), dan semua Pengarah Jabatan.	YDP, CDO, ICTSO, Pengarah Jabatan

010102 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna ICT MPS (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO

010103 Penyelenggaraan Dasar

Dasar Keselamatan ICT MPS 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 Dasar Keselamatan ICT MPS: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk dibentangkan dan diluluskan oleh pengurusan melalui Mesyuarat Pengurusan / Mesyuarat Jawatankuasa Perkhidmatan dan Teknologi Maklumat (JPTM) / mesyuarat yang setara; (c) Maklum kepada semua pengguna yang berkaitan berkenaan perubahan yang telah dipersetujui oleh Mesyuarat Pengurusan / JPTM / mesyuarat yang setara; dan	ICTSO

(d) Dasar Keselamatan ICT MPS ini perlu dikaji semula sekurang-kurangnya dua tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	
010104 Pengecualian Dasar	
(a) Permohonan pengecualian dasar keselamatan ICT dan prosedur ICT boleh dibuat dengan melengkapkan borang Permohonan Pengecualian Pematuhan Dasar Keselamatan ICT beserta justifikasi dan faedah yang dikaitkan dengan penafian. Permohonan pengecualian ini perlu mendapat kelulusan daripada CDO atau ICTSO. Pengecualian Dasar Keselamatan ICT ini adalah merujuk kepada polisi ISMS dan hanya boleh digunakan dalam situasi yang berkaitan untuk tempoh masa maksimum satu (1) tahun. Pengecualian polisi perlu dinilai semula apabila tamat tempoh satu (1) tahun atau tempoh yang dirasakan sesuai. (b) Permohonan pengecualian dasar ini perlu dimohon dengan menggunakan borang **Permohonan Pengecualian Pematuhan DKICT MPS** seperti di **Lampiran 1**.	Semua

BIDANG 02
ORGANISASI KESELAMATAN

0201 INFRASTRUKTUR ORGANISASI DALAMAN

Objektif :

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT MPS.

020101 Yang Dipertua, MPS

Yang Dipertua MPS adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MPS; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MPS; (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 Dasar Keselamatan ICT MPS; dan (e) Mempengerusikan Mesyuarat Pengurusan / Mesyuarat Jawatankuasa Perkhidmatan dan Teknologi Maklumat.	YDP

020102 Ketua Pegawai Digital (Chief Digital Officer - CDO)

Ketua Pegawai Digital (CDO) bagi MPS ialah Timbalan Yang Dipertua MPS. Peranan dan tanggungjawab CDO adalah seperti berikut: (a) Membantu Yang Dipertua dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan keselamatan ICT; dan (c) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPS.	CDO

020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi MPS ialah Pengarah Teknologi Maklumat. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT MPS; (b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT MPS; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MPS kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPS; (e) Menjalankan pengurusan risiko; (f) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (g) Melaporkan insiden keselamatan ICT kepada Pengurusan Tertinggi MPS. (h) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; (i) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; (j) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan (k) Menyelaras dan mengurus pelan latihan keselamatan ICT.	ICTSO
020104 Pegawai Aset ICT	
Pegawai Aset ICT bagi MPS ialah pegawai yang menguruskan peralatan dan aksesori ICT. Peranan dan tanggungjawab Pegawai Aset ICT adalah seperti berikut:	Pegawai Aset ICT

(a) Menentukan kawalan akses pengguna terhadap aset ICT MPS; (b) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; (c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT; (e) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPS; dan (f) Bertindak sebagai pegawai yang menguruskan asset-aset ICT Majlis.	
020105 Pentadbir Sistem ICT	
Pentadbir Sistem ICT bagi MPS ialah pegawai yang menguruskan aplikasi di MPS. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (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 Dasar Keselamatan ICT MPS; (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) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; (f) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPS; dan	Pentadbir Sistem ICT

(g) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPS.	
020106 Pentadbir Pusat Data / Rangkaian	
Pentadbir Pusat Data / Rangkaian ialah Pegawai yang dipertanggungjawabkan mentadbir Pusat Data MPS dan seterusnya melaksanakan pematuhan DKICT MPS. Pentadbir Pusat Data / Rangkaian mempunyai peranan dan tanggungjawab seperti berikut:- (a) Menyediakan dan melaksana garis panduan, prosedur dan tatacara pentadbiran Pusat Data selaras dengan keperluan DKICT MPS; (b) Memastikan Pusat Data MPS beroperasi sepanjang masa; (c) Memastikan keselamatan fizikal dan persekitaran Pusat Data MPS sentiasa dlam keadaan baik dan mengambil langkah-langkah untuk mengurangkan risiko ancaman keselamatan ICT bagi melindungi perkhidmatan di Pusat Data; (d) Bertanggungjawab memantau setiap perkakasan dan perisian ICT yang ditempatkan di Pusat Data di dalam keadaan yang baik; (e) Memantau dan mengawal akses fizikal (keluar dan masuk) ke Pusat Data; (f) Mengawal dan memantau capaian secara atas talian ke server-server dan peralatan ICT di Pusat Data seperti penyediaan *Console Room*, buku log dan sebagainya; (g) Memantau aktiviti capaian perkhidmatan di Pusat Data dan melaporkan kepada ICTSO dengan segera sekiranya berlaku sebarang insiden pelanggaran dasar keselamatan Pusat Data; (h) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di MPS beroperasi sepanjang masa; (i) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; (j) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO dengan segera sekiranya berlaku penyalahgunaan penggunaan rangkaian; dan	Pentadbir Pusat Data / Rangkaian

(k) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian MPS secara tidak sah seperti melalui peralatan modem dan *dial-up* tanpa kebenaran;	
020107 Pengguna	
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPS; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; (d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MPS dan menjaga kerahsiaan maklumat MPS; (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 Dasar Keselamatan ICT MPS** sebagaimana di **Lampiran 2**; dan (h) Melaksanakan langkah-langkah perlindungan seperti berikut: 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 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 maklumat-maklumat terperingkat berkaitan keselamatan ICT.	Pengguna

020108 Jawatankuasa Perkhidmatan dan Teknologi Maklumat (JPTM)	
Jawatankuasa Perkhidmatan dan Teknologi Maklumat (JPTM) adalah jawatankuasa yang bertanggungjawab dalam meluluskan dan berperanan sebagai penasihat dan membentangkan projek baru ICT. Keanggotaan JPTM MPS adalah seperti berikut: Pengerusi : YDP MPS Ahli : (1) Timbalan Yang Dipertua (CDO) (2) ICTSO MPS (3) Semua Pengarah dan Ketua Bahagian (4) Ahli Majlis Bidang kuasa: (a) Menetapkan arah tuju dan strategi untuk pelaksanaan ICT MPS; (b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arahtuju/strategi ICT MPS; (c) Merancang dan menentukan langkah-langkah keselamatan ICT; (d) Mengikuti dan memantau perkembangan program ICT MPS dan Jabatan di bawahnya, serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT; (e) Menilai dan meluluskan semua perolehan ICT MPS dan Jabatan di bawahnya berdasarkan keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan; dan (f) Menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi MPS dan Jabatan di bawahnya.	JPTM MPS
020109 Jawatankuasa Teknikal ICT MPS	
Jawatankuasa Teknikal ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MPS.	JKICT, MPS

Keanggotaan JKICT MPS adalah seperti berikut:

Pengerusi : Timbalan Yang Dipertua

Ahli :

(1) Jabatan Perundangan
(2) Jabatan Perbendaharaan
(3) Jabatan Khidmat Pengurusan
(4) Jabatan Penilaian & Pengurusan Harta
(5) Jabatan Pengurusan Sisa Pepejal dan Kesihatan
(6) Jabatan Audit Dalam
(7) Jabatan Kontrak dan Ukur Bahan
(8) Jabatan Kejuruteraan
(9) Jabatan Korporat
(10) Jabatan yang terlibat dengan projek ICT

Urus Setia bagi JKICT MPS ialah Jabatan Teknologi Maklumat.

Bidang kuasa:

(a) Memperakukan dokumen DKICT MPS;

(b) Sebagai penasihat bagi projek-projek ICT yang akan dilaksanakan;

(c) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan projek ICT;

(d) Menerima laporan dan membincangkan hal-hal berkaitan projek ICT semasa; dan

(e) Membuat keputusan mengenai tindakan yang perlu diambil berkenaan projek ICT.

0202 PIHAK KETIGA

Objektif:

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

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Pihak ketiga terdiri daripada kontraktor, pembekal dan penyedia perkhidmatan luaran. Peranan dan tanggungjawab pihak ketiga adalah bertujuan bagi memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal sama ada untuk pelaksanaan projek ICT atau tindakan *outsource* perkhidmatan tertentu. Perkara yang perlu dipatuhi oleh pihak ketiga termasuk yang berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPS; (b) Melakukan akses ke atas aset ICT MPS berdasarkan kepada perjanjian kontrak; (c) Menandatangani **Surat Akuan Pematuhan Dasar Keselamatan ICT MPS** (**Lampiran 2)** dan ***Non-disclosure Agreement*** **(NDA) (Lampiran 3)**; (d) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran akses kepada pihak ketiga; (e) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (f) Akses kepada aset ICT MPS perlu berlandaskan kepada perjanjian kontrak; (g) Memahami implikasi keselamatan ke atas sebarang tindakan yang dilakukan; dan (h) Melaporkan dengan segera sebarang aktiviti atau keadaan yang meragukan yang mungkin memberikan ancaman kepada aset ICT.	CDO, ICTSO, Pegawai Aset ICT, Pentadbir Sistem ICT, Pentadbir Pusat Data / Rangkaian dan Pihak Ketiga

BIDANG 03
PENGURUSAN ASET

0301 AKAUNTABILITI ASET

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MPS

030101 Inventori Aset ICT

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam kad 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 MPS; (d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai Aset ICT dan Pengguna

0302 PENGELASAN DAN PENGENDALIAN MAKLUMAT

Objektif:

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

030201 Pengelasan Maklumat

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan ICT. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	Pegawai Pengelas Maklumat

030202 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 ada untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

BIDANG 04
KESELAMATAN SUMBER MANUSIA

0401 KESELAMATAN SUMBER MANUSIA DALAM TUGAS HARIAN

Objektif:

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

040101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MPS serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPS yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan; dan (d) Memenuhi keperluan prosedur keselamatan (menandatangani NDA) bagi pembekal, pakar runding, pihak ketiga dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan ICT atau yang berkaitan dengan keselamatan ICT.	Semua

040102 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut : (a) Memastikan pegawai dan kakitangan MPS serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MPS;	Semua

(b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPS 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 MPS serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MPS; 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 Jabatan Teknologi Maklumat dan Unit Latihan, Jabatan Khidmat Pengurusan.	
040103 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada MPS mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MPS dan/atau terma perkhidmatan.	Semua

BIDANG 05
KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 KESELAMATAN KAWASAN

Objektif:

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

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: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas; (b) Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (c) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (d) Memasang alat penggera atau kamera; (e) Menghadkan jalan keluar masuk; (f) Mewujudkan kawalan keselamatan; (g) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (h) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (i) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;	CDO, ICTSO, Pengarah, Pentadbir Pusat Data / Rangkaian

(j) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (k) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap kakitangan MPS (bukan yang dibenarkan) dan pihak ketiga perlu mengisi buku pelawat masuk/keluar ke Jabatan Teknologi Maklumat; dan (b) Kakitangan MPS dan pihak ketiga yang hendak berurusan dengan Pusat Data haruslah mendapatkan kebenaran daripada ICTSO atau Pentadbir Pusat Data/Rangkaian melalui Borang Kebenaran Kerja dan perlu mengisi Rekod Masuk Keluar Pusat Data	Semua
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. Kawasan larangan di MPS adalah bilik Yang Dipertua, bilik Timbalan Yang Dipertua/Setiausaha, Pusat Data (*Data Centre*), Bilik Server, Bilik Rangkaian, Bilik Kebal, Bilik Fail, semua Stor dan mana-mana kawasan yang diisytiharkan sebagai kawasan larangan. (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 diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Semua

0502 KESELAMATAN PERALATAN

Objektif:

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

050201 Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (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 Pengarah Teknologi Maklumat; (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; (h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian dan kerosakan; (i) Penyalahgunaan atau pengubahsuaian tanpa kebenaran adalah dilarang; (j) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); (k) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switch*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;	Semua

(l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (m) Peralatan ICT yang hendak dibawa keluar dari premis MPS, Borang Kebenaran Membawa Keluar Peralatan ICT hendaklah diisi dan mendapatkan kebenaran dari Pengarah atau Pegawai Aset ICT; (n) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Unit Pengurusan Aset Alih MPS dengan segera; (o) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (p) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset ICT; (q) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Unit Aduan, Jabatan Teknologi Maklumat untuk dibaikpulih; (r) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (s) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (u) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF” apabila meninggalkan pejabat; (v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan (w) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *CDROM, DVDROM*, *thumb drive, external hard disk* dan media storan lain.	Semua

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) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (e) Akses dan pergerakan media storan hendaklah direkodkan; (f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; (g) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan (h) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MPS; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran ICTSO; dan (c) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua

050204 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. 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; dan (e) Sekiranya perlu, memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan.	Pegawai Aset ICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data / Rangkaian
050205 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis MPS adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian	Semua
050206 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang , tidak boleh dibaiki dan tidak ekonomi untuk dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MPS dan ditempatkan di MPS. Peralatan ICT yang hendak dilupuskan perlu merujuk tatacara yang terdapat pada pekeliling 1PP. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPS.	Semua, Pegawai Aset ICT dan ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing,* pemusnahan media storan atau pembakaran;

(b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat salinan penduaan;

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

(d) Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

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

(f) Pegawai Aset ICT bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam kad KEW PA 3, KEW PA 4 dan di dalam Sistem e-Aset;

(g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

(h) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.

ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM, hardisk, motherboard* dan sebagainya;

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

iv. Memindah keluar dari MPS mana-mana peralatan ICT yang hendak dilupuskan; dan

v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MPS.

0503 KESELAMATAN PERSEKITARAN

Objektif:

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

050301 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Yang Dipertua/Timbalan Yang Dipertua atau Jawatankuasa Teknikal ICT, MPS. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan Pusat Data (peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkap dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran; (c) Peralatan perlindungan hendaklah dipasang ditempat 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; dan (g) Semua peralatan perlindungan hendaklah diselenggara secara berkala. Aktiviti ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	Semua

050302 Bekalan Kuasa

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

(a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; dan (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan.	

050303 Kabel

Kabel komputer 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.	Semua

050304 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Prosedur kecemasan dengan merujuk kepada proses kerja pengurusan kecemasan yang ditetapkan oleh Jawatankuasa Keselamatan dan Kesihatan Pekerjaan (JKKP) MPS; dan

(b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada wakil yang dilantik mengikut aras.

0504 KESELAMATAN DOKUMEN

Objektif:

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

050401 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difailkan mengikut klasifikasi keselamatan sama ada Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut tatacara kawalan dokumen yang telah ditetapkan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan kepada Ketua Jabatan mengikut Arahan Keselamatan; dan (d) Pelupusan dokumen hendaklah mengikut tatacara Arahan Keselamatan dan juga garis panduan dari Jabatan Arkib Negara.	Semua

BIDANG 06
PENGURUSAN OPERASI DAN KOMUNIKASI

0601 PENGURUSAN PROSEDUR OPERASI

Objektif:

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

060101 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (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.	Semua

060102 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur perlulah mengikut prosedur yang telah ditetapkan; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (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 sengaja.	Semua

060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Semua

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.

060201 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (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; dan (c) Sebarang perubahan perkakasan dan perisian yang dilaksanakan oleh pihak ketiga perlu mengambil kira tahap kritikal persekitaran serta proses-proses yang teribat.	Semua

0603 PERANCANGAN DAN PENERIMAAN SISTEM

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

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. 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.	ICTSO, Pentadbir Sistem ICT dan Pentadbir Pusat Data / Rangkaian

060302 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	ICTSO dan Pentadbir Sistem ICT

0604 PERISIAN BERBAHAYA

Objektif:

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

060401 Perlindungan dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus 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 fail di dalam *removable drive* seperti *external hard disk* dan *pen drive* sebelum digunakan di peralatan komputer MPS;	Semua

(d) Mengemas kini antivirus dengan pattern anti virus yang terkini; (e) Menyemak kandungan sistem atau maklumat 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 berisiko terhadap perisian; dan (h) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
060402 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan sama sekali melainkan dengan kebenaran Pengarah Teknologi Maklumat, MPS.	Semua
0605 HOUSEKEEPING	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501 *Backup*	
Backup hendaklah dilakukan secara berjadual atau setiap kali konfigurasi berubah bagi memastikan sistem dapat dipulihkan semula setelah berlakunya bencana atau berdasarkan keperluan. 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;	ICTSO, Pentadbir Sistem ICT dan Pentadbir Pusat Data / Rangkaian

(c) Menguji sistem *backup* dan *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan (d) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	

0606 PENGURUSAN RANGKAIAN.

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

060601 Kawalan Infrastruktur Rangkaian

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; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Pemasangan firewall untuk mengawal capaian ke atas sistem yang telah dibangunkan dan memastikan keselamatan aset ICT dalam rangkaian dari pencerobohan; (e) Semua pengguna hanya dibenarkan menggunakan rangkaian MPS sahaja. Penyambungan rangkaian melalui modem, router, telefon dan lain-lain persendirian adalah dilarang sama sekali; (f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MPS; (g) Larangan memuat turun perisian berbahaya bagi mengelakkan prestasi rangkaian terganggu dan mengelakkan penyebaran virus;	ICTSO dan Pentadbir Pusat Data / Rangkaian

(h) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; dan (i) Kemudahan bagi wireless LAN perlu dipastikan kawalan keselamatan.	

0607 PENGURUSAN MEDIA

Objektif:

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

060701 Prosedur Pengendalian Media

Prosedur-prosedur pengendalian media yang perlu dipatuhi dalam peminjaman media adalah seperti berikut: (a) Memastikan media yang akan dipinjam dikelaskan mengikut tahap sensitiviti sesuatu maklumat seperti Prosedur Klasifikasi dan Pengendalian Maklumat; (b) Mendapatkan kelulusan peminjaman media melalui Borang Permohonan Pinjaman Peralatan ICT; (c) Sekiranya media / peralatan dibawa keluar, Borang Kebenaran Membawa Keluar Peralatan ICT perlu diisi; (d) Peminjaman direkodkan menggunakan Daftar Pergerakan Harta Modal & Inventori (KEW PA-9); (e) Media yang dipinjam atau dibawa keluar dari pejabat, perlu merujuk kepada Prosedur Klasifikasi dan Pengendalian Maklumat bagi pengendalian maklumat yang terdapat di dalam media; (f) Media yang dipulangkan mestilah berada di dalam keadaan yang baik dan direkodkan; (g) Pegawai bertukar atau bersara perlu menyerahkan kembali media yang digunakan; dan (h) Memastikan media adalah selamat daripada kod perosak	Semua / Pegawai Aset ICT

Bagi pengurusan penyimpanan media pula: (a) Memastikan media disimpan dalam persekitaran yang selamat dan dilabelkan mengikut pengelasannya seperti Prosedur Klasifikasi dan Pengendalian Maklumat; (b) Sekiranya media yang digunakan telah melangkaui jangka hayatnya, kandungan fail atau maklumat di dalamnya perlulah dipindahkan ke media lain; dan (c) Sekiranya data atau maklumat dalam media tidak lagi diperlukan, data atau maklumat tersebut perlu dipadamkan secara selamat dan tidak boleh dibaik pulih (*unrecoverable*). Tindakan pelupusan media perlu mengikut tatacara yang telah ditetapkan di dalam Tatacara Pengurusan Aset Alih Kerajaan : Pelupusan.	
060702 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: (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.	Semua
0608 PENGURUSAN PEMINDAHAN MAKLUMAT	
Objektif: Memastikan keselamatan pemindahan maklumat antara MPS dan agensi luar terjamin.	
060801 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;	Semua

(b) Mendapatkan persetujuan pihak penerima maklumat bagi melaksanakan kawalan ke atas maklumat terperingkat melalui e-mel / surat / memo (*disclaimer*); (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MPS; dan (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	
060802 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di MPS hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam 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. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MPS sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MPS; (c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; (d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; (e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; (f) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;	Semua

(g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mail; (h) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (i) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; (j) Memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan dengan kadar segera; (k) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti *yahoo.com, gmail.com, streamyx.com.my* dan sebagainya) tidak digunakan untuk tujuan rasmi. Sekiranya pengguna menggunakan e-mel persendirian untuk tujuan rasmi, MPS tidak akan bertanggungjawab ke atas sebarang insiden yang berlaku; dan (l) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	

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.

060901 E-Dagang

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

(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.	
060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (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.	Jabatan Teknologi Maklumat
0610 PEMANTAUAN	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan	
061001 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT MPS; (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);	ICTSO

(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) selain daripada yang telah diperuntukkan tanpa kebenaran Pengarah Teknologi Maklumat, MPS.	
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. 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 sekurang-kurangnya lima (5) tahun. 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.	Pentadbir Sistem ICT

Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
061003 Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada CDO dan ICTSO.	Pentadbir Sistem ICT
061004 Pemantauan Log	
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 MPS atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pentadbir Sistem ICT dan Pentadbir Pusat Data / Rangkaian

BIDANG 07
KAWALAN CAPAIAN

0701 DASAR KAWALAN CAPAIAN

Objektif:

Mengawal capaian ke atas maklumat

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. 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 mudahalih dan; (d) Kawalan ke atas kemudahan pemprosesan maklumat.	Jabatan Teknologi Maklumat

0702 PENGURUSAN CAPAIAN PENGGUNA

Objektif:

Mengawal capaian pengguna ke atas aset ICT MPS

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: (a) Akaun yang diperuntukkan oleh MPS sahaja boleh digunakan;	Semua dan Pentadbir Sistem ICT

(b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Tahap capaian akaun pengguna yang diwujudkan akan diberikan mengikut permohonan dan telah diluluskan daripada pemilik sistem. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MPS. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (f) Pentadbir – pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan	
070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
070203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik yang ditetapkan oleh MPS 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; dan (c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara, dan mesti terdiri daripada kombinasi huruf dan nombor, atau simbol khas.	Semua dan Pentadbir SIstem ICT

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. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna, papan putih *(white board)* atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *logout* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat; dan (d) Memastikan tiada maklumat-maklumat sensitif di atas papan putih selepas digunakan.	Semua

0703 KAWALAN CAPAIAN RANGKAIAN

Objektif:

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

070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang firewall yang bersesuaian di antara rangkaian MPS dan rangkaian luar; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO dan Pentadbir Pusat Data / Rangkaian

070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di MPS hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja; (b) Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code, virus* dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MPS; (c) *Kaedah Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (d) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; (e) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. ICTSO berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; (f) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah/Ketua Bahagian yang diberi kuasa; (g) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet; (h) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MPS; (i) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CDO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; (j) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan	ICTSO dan Pentadbir Pusat Data / Rangkaian

(k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian yang meragukan dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	

0704 KAWALAN CAPAIAN SISTEM PENGOPERASIAN

Objektif:

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

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. 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: i. Mengesahkan pengguna yang dibenarkan; ii. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user* 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) Menghadkan dan mengawal penggunaan program; dan (d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi bagi tempoh 15 minit.	ICTSO dan Pentadbir Sistem ICT

0705 KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT

Objektif:

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

070501 Capaian Aplikasi dan Maklumat

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 (*system log*); (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 dihadkan kepada perkhidmatan yang dibenarkan sahaja; (e) Capaian kepada kod sumber aturcara (*programmesource code*) hendaklah dihadkan; (f) Pengguna dan Pembekal/kontraktor penyelenggaraan yang memerlukan akaun bagi mendapat capaian ke sistem-sistem di MPS perlu mendapatkan kebenaran daripada Pentadbir Sistem ICT; dan (g) Pengguna dan Pembekal/kontraktor penyelenggaraan bertanggungjawab untuk memaklumkan Pentadbir Sistem ICT sekiranya tidak memerlukan akaun lagi bagi tujuan capaian kepada sistem.	ICTSO dan Pentadbir Sistem ICT

0706 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH

Objektif:

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

070601 Peralatan Mudah Alih

Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua

070602 Kerja Jarak Jauh

Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

BIDANG 08
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 KESELAMATAN DALAM MEMBANGUNKAN SISTEM DAN APLIKASI

Objektif:

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

080101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) 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; (c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; (d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; dan	ICTSO dan Pentadbir Sistem ICT

080102 Pengesahan Data *Input* dan *Output*

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (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.	Pemilik Sistem dan Pentadbir Sistem ICT

0802 KAWALAN KRIPTOGRAFI

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

080201 Enkripsi

Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua

080202 Pengurusan Infrastruktur Kunci Awam (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.	Pentadbir Sistem ICT

0803 KESELAMATAN FAIL SISTEM

Objektif:

Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat

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; (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 pengemaskini untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem dan Pentadbir Sistem ICT

0804 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

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 penambahbaikan dan pembetulan yang dilakukan oleh vendor; (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 diizinkan; dan (e) Menghalang sebarang peluang untuk membocorkan maklumat.	Pemilik Sistem dan Pentadbir Sistem ICT

080402 Pembangunan Perisian Secara *Outsource*

Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik MPS.	Pentadbir Sistem ICT

0805 KAWALAN TEKNIKAL KETERDEDAHAN (*VULNERABILITY*)

Objektif:

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

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; (b) Menilai tahap keterdedahan (*Security Posture Assessment*) bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	ICTSO dan Pentadbir Sistem ICT

BIDANG 09
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 MEKANISME PELAPORAN INSIDEN KESELAMATAN ICT

Objektif:

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

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 dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CDO dengan kadar segera: Perkara-perkara yang perlu dilaporkan adalah seperti berikut : (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 MPS sepertimana Lampiran 4. Prosedur pelaporan insiden keselamatan ICT berdasarkan:	Semua

(a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	

0902 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT

Objektif :

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

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 MPS. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

BIDANG 10
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 DASAR KESINAMBUNGAN PERKHIDMATAN

Objektif:

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

100101 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKICT MPS. Perkara-perkara berikut perlu diberi perhatian: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (f) Membuat backup; dan (g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;	CDO, ICTSO, Pentadbir Sistem ICT dan Pentadbir Pusat Data / Rangkaian

(b) Senarai personel MPS dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). (c) Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; (d) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (e) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (f) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. 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 personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. MPS hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

BIDANG 11
PEMATUHAN

1101 PEMATUHAN DAN KEPERLUAN PERUNDANGAN

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MPS.

110101 Pematuhan Dasar

Setiap pengguna di MPS hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MPS dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di MPS termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. ICTSO/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT MPS selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MPS.	Semua

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

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

110104 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di MPS adalah seperti di **Lampiran 5.**	Semua
110105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT MPS boleh dikenakan tindakan displin perundangan majlis seperti tindakan tatatertib.	Semua

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti *hard disk*, *external hard disk* dan *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CDO	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
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*).
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (*hub)* merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, 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 rangkaianrangkaian 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.
Logout	Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.

MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
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.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer

Switch	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.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

PERMOHONAN PENGECUALIAN PEMATUHAN

DASAR KESELAMATAN ICT MPS

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Jabatan / Bahagian : ……

Bidang	Butiran Pengecualian	Justifikasi

Tempoh Pengecualian : Tarikh Mula …… - Tarikh Tamat …….

**Tempoh maksima yang dibenarkan adalah selama satu (1) tahun sahaja.*

Pengesahan dan Kelulusan

Ulasan : ……..

……

***Diluluskan / Tidak diluluskan.**

..... Tarikh: ……..

( )

b.p. Yang Dipertua, MPS

Lampiran 2

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT MPS

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Jabatan / Bahagian : ……
(untuk staf MPS sahaja)

Nombor Pekerja : ……..
(untuk staf MPS sahaja)

Syarikat : ……..
(selain staf MPS sahaja)

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT MPS; 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 (ICTSO)

.....

( )

b.p. Yang Dipertua, MPS

Tarikh: .....

Lampiran 3

PERJANJIAN KERAHSIAAN *(NON-DISCLOSURE AGREEMENT)*

NAMA PROJEK :

Saya …… bernombor kad pengenalan ……..…

berjawatan ……...… dari Syarikat ……..…..……

dengan ini:

(a) tidak mendedahkan sebarang maklumat dan memberi perlindungan kerahsiaan yang sewajarnya kepada semua maklumat mengenai projek ini;

(b) 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 mengenai projek ini;

(c) tidak mempunyai kepentingan peribadi terhadap projek ini;

(d) Saya 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 suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

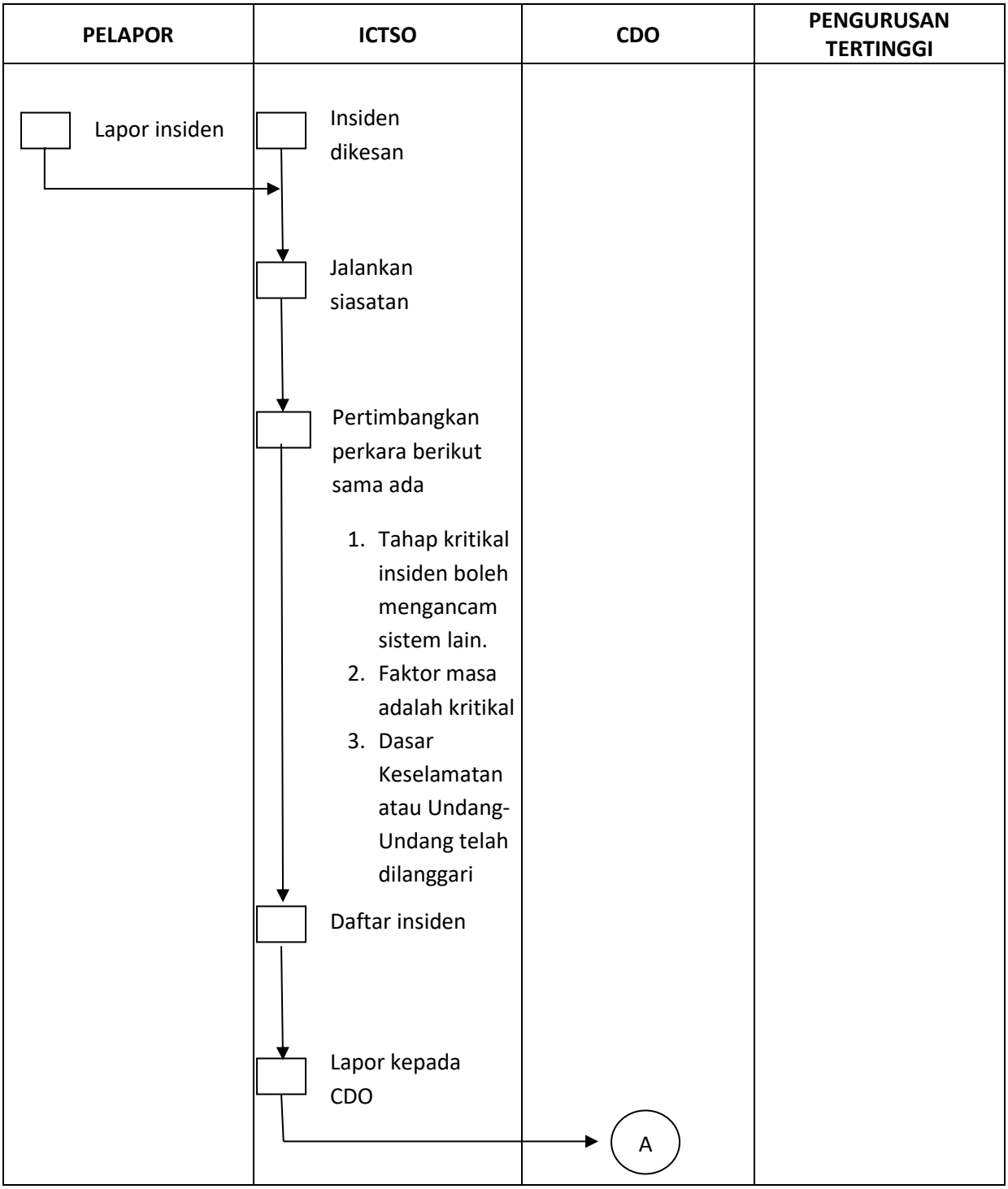
(e) Saya juga memahami dan bersedia untuk diambil tindakan, sekiranya Jabatan Teknologi Maklumat (JTM), Majlis Perbandaran Selayang mendapati saya melanggar perjanjian yang telah ditandatangani ini

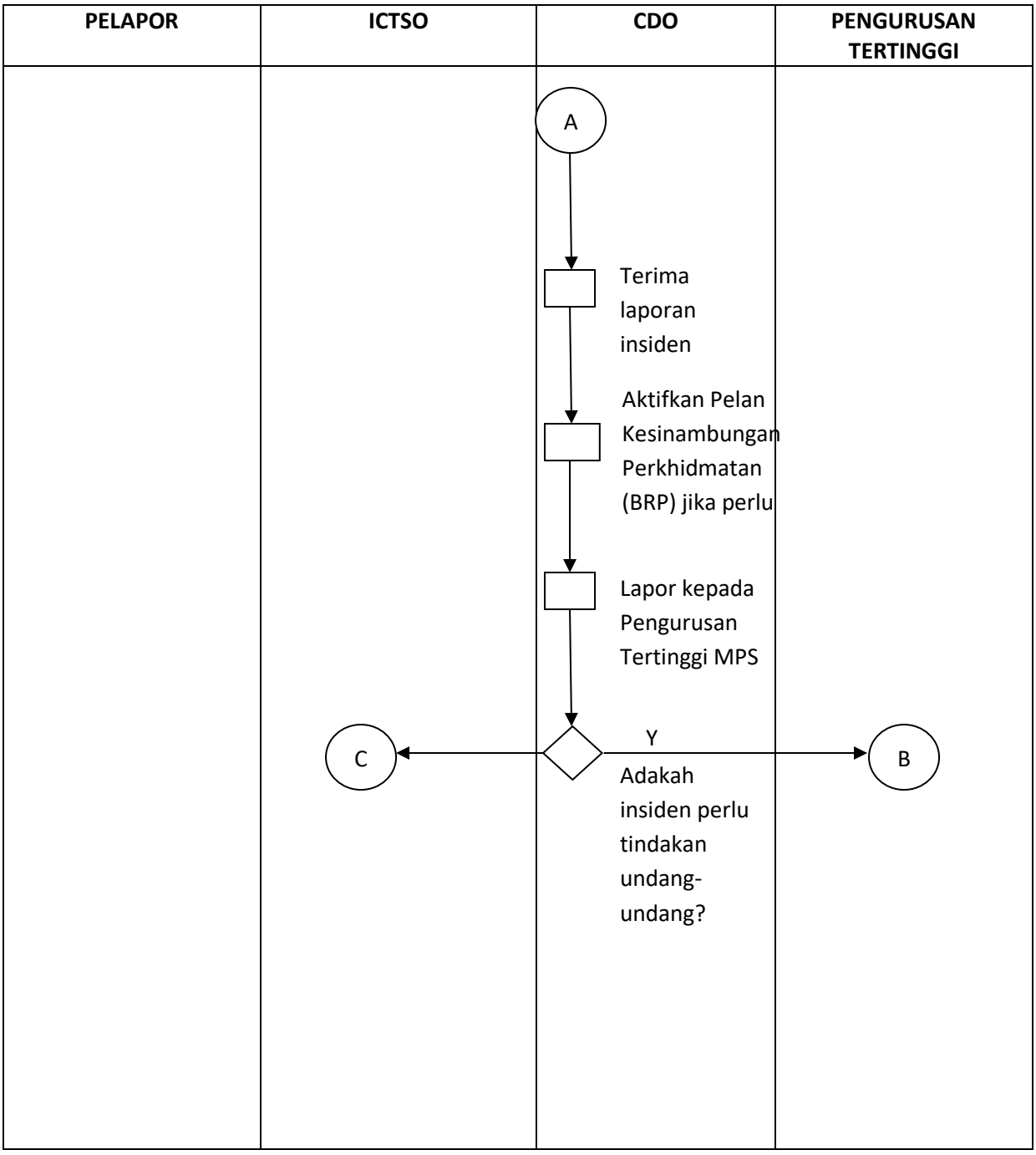
....

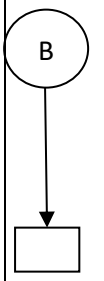
(Tandatangan) (Tarikh)

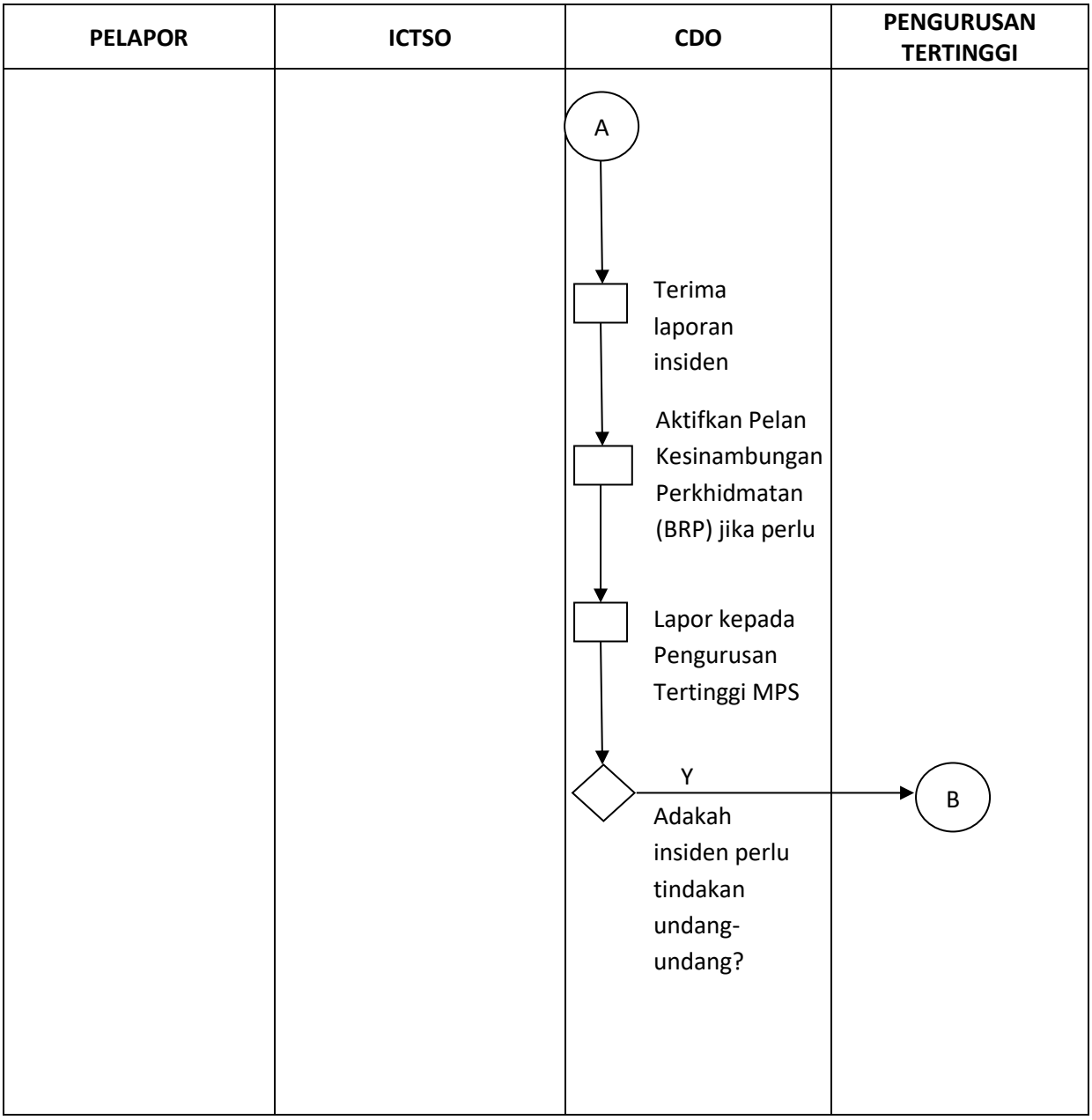
Lampiran 4

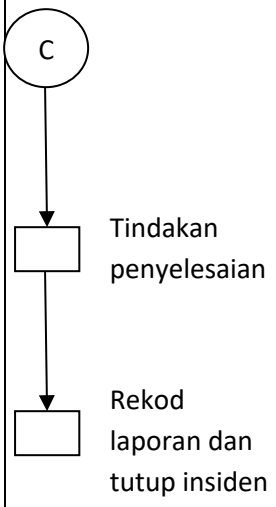
Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT MPS




PELAPOR
ICTSO
CDO
PENGURUSAN TERTINGGI
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada Pengurusan Tertinggi MPS
Y
Adakah insiden perlu tindakan undang-undang?
C
B

PELAPOR	ICTSO	CDO	PENGURUSAN TERTINGGI
		 Ambil tindakan ke atas insiden yang menyalahi undang-undang dan peraturan berkaitan	


PELAPOR
ICTSO
CDO
PENGURUSAN TERTINGGI
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada Pengurusan Tertinggi MPS
Y
Adakah insiden perlu tindakan undang-undang?
B

PELAPOR	ICTSO	CDO	PENGURUSAN TERTINGGI
			

Lampiran 5

SENARAI PERUNDANGAN DAN PERATURAN

1) Arahan Keselamatan;

2) Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

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

4) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT);

5) Pekeliling Kemajuan Penradbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;

6) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

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

8) 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;

9) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

10) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi – Agensi Kerajaan yang bertarikh 23 November 2007;

11) Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa – jawatankuasa di bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

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

13) Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundangan;

14) Akta Tandatangan Digital 1997;

15) Akta Rahsia Rasmi 1972;

16) Akta Jenayah Komputer 1997;

17) Akta Hak Cipta (Pindaan) Tahun 1997;

18) Akta Komunikasi dan Multimedia 1998;

19) Perintah – Perintah Am;

20) Arahan Perbendaharaan;

21) Arahan Teknologi Maklumat 2007;

22) Garis Panduan Keselamatan MAMPU 2004;

23) *Standard Operating Procedure* (SOP) ICT MPS;

24) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

25) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.

26) *Standard Operating Procedure* (SOP) AM Perintah Kawalan Pergerakan

JABATAN TEKNOLOGI MAKLUMAT
MAJLIS PERBANDARAN SELAYANG