



MAJLIS PERBANDARAN SEPANG

DASAR KESELAMATAN ICT

VERSI 2.1

10 DISEMBER 2015

ISI KANDUNGAN

PENGENALAN	1
OBJEKTIF	1
PERNYATAAN DASAR	2
SKOP	4
PRINSIP-PRINSIP	6
PERKARA 01 - PEMBANGUNAN DAN PENYELENGGARAAN DASAR	15
0101 Dasar Keselamatan ICT	15
010101 Pelaksanaan Dasar	15
010102 Penyebaran Dasar	15
010103 Penyelenggaraan Dasar	15
010104 Pengecualian Dasar	16
PERKARA 02 - ORGANISASI KESELAMATAN	17
0201 Infrastruktur Organisasi Dalaman	17
020101 Yang Dipertua MPSEPANG	17
020102 Ketua Pegawai Maklumat (CIO)	17
020103 Pegawai Keselamatan ICT (ICTSO)	18
020104 Pengurus ICT	19
020105 Pentadbir Sistem ICT	19
020106 Pengguna	20
020107 Jawatan Kuasa Keselamatan ICT MPSEPANG	21
020108 Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan	

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	18/08/15	ii

(GCERT)	22
0202 Pihak Ketiga	23
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	23
PERKARA 03 - PENGURUSAN ASET	25
0301 Akauntabiliti Aset	25
030101 Inventori Aset ICT	25
0302 Pengelasan dan Pengendalian Maklumat	26
030201 Pengelasan Maklumat	26
030202 Pengendalian Maklumat	26
PERKARA 04 - KESELAMATAN SUMBER MANUSIA	28
0401 Keselamatan Sumber Manusia Dalam Tugas Harian	28
040101 Sebelum Perkhidmatan	28
040102 Dalam Perkhidmatan	28
040103 Bertukar Atau Tamat Perkhidmatan	29
PERKARA 05 - KESELAMATAN FIZIKAL DAN PERSEKITARAN	30
0501 Keselamatan Kawasan	30
050101 Kawalan Kawasan	30
050102 Kawalan Masuk Fizikal	31
050103 Kawasan Larangan	31
0502 Keselamatan Peralatan	32
050201 Peralatan ICT	32

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	18/08/15	iii

050202 Media Storan	34
050203 Media Tandatangan Digital	35
050204 Media Perisian dan Aplikasi	35
050205 Penyelenggaraan Perkakasan	36
050206 Peralatan di Luar Premis	36
050207 Pelupusan Perkakasan	37
0503 Keselamatan Persekitaran	38
050301 Kawalan Persekitaran	38
050302 Bekalan Kuasa	39
050303 Kabel	40
050304 Prosedur Kecemasan	40
0504 Keselamatan Dokumen	41
050401 Dokumen	41
PERKARA 06 - PENGURUSAN OPERASI DAN KOMUNIKASI	42
0601 Pengurusan Prosedur Operasi	42
060101 Pengendalian Prosedur	42
060102 Kawalan Perubahan	42
060103 Pengasingan Tugas dan Tanggungjawab	43
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	44
060201 Perkhidmatan Penyampaian	44
0603 Perancangan dan Penerimaan Sistem	44
060301 Perancangan Kapasiti	44
060302 Penerimaan Sistem	45

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	18/08/15	iv

0604 Perisian Berbahaya	45
060401 Perlindungan dari Perisian Berbahaya	45
060402 Perlindungan dari Mobile Code	46
0605 Housekeeping	46
060501 Backup	46
0606 Pengurusan Rangkaian	47
060601 Kawalan Infrastruktur Rangkaian	47
0607 Pengurusan Media	48
060701 Penghantaran dan Pemindahan	48
060702 Prosedur Pengendalian Media	48
060703 Keselamatan Sistem Dokumentasi	49
0608 Pengurusan Pertukaran Maklumat	49
060801 Pertukaran Maklumat	49
060802 Pengurusan Mel Elektronik (E-mel)	50
0609 Perkhidmatan E-Dagang (Electronic Commerce Services)	51
060901 E-Dagang	51
060902 Maklumat Umum	52
0610 Pemantauan	52
061001 Pengauditan dan Forensik ICT	52
061002 Jejak Audit	53
061003 Sistem Log	54
061004 Pemantauan Log	54

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	18/08/15	v

PERKARA 07 - KAWALAN CAPAIAN	56
0701 Dasar Kawalan Capaian	56
070101 Keperluan Kawalan Capaian	56
0702 Pengurusan Capaian Pengguna	56
070201 Akaun Pengguna	56
070202 Hak Capaian	57
070203 Pengurusan Kata Laluan	57
070204 Clear Desk dan Clear Screen	58
0703 Kawalan Capaian Rangkaian	59
070301 Capaian Rangkaian	59
070302 Capaian Internet	59
0704 Kawalan Capaian Sistem Pengoperasian	61
070401 Capaian Sistem Pengoperasian	61
070402 Kad Pintar	62
0705 Kawalan Capaian Aplikasi dan Maklumat	63
070501 Capaian Aplikasi dan Maklumat	63
0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	64
070601 Peralatan Mudah Alih	64
070602 Kerja Jarak Jauh	64

PERKARA 08 - PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM **65**

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi	65
080101 Keperluan Keselamatan Sistem Maklumat	65

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	18/08/15	vi

080102 Pengesahan Data Input dan Output	65
0802 Kawalan Kriptografi	66
080201 Enkripsi	66
080202 Tandatangan Digital	66
080203 Pengurusan Infrastruktur Kunci Awam (PKI)	66
0803 Keselamatan Fail Sistem	66
080301 Kawalan Fail Sistem	66
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan	67
080401 Prosedur Kawalan Perubahan	67
080402 Pembangunan Perisian Secara Outsource	68
0805 Kawalan Teknikal Keterdedahan (Vulnerability)	68
080501 Kawalan dari Ancaman Teknikal	68

PERKARA 09 - PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

	69
0901 Mekanisme Pelaporan Insiden Keselamatan ICT	69
090101 Mekanisme Pelaporan	69
0902 Pengurusan Maklumat Insiden Keselamatan ICT	70
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	70

PERKARA 10 - PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan	72
100101 Pelan Kesinambungan Perkhidmatan	72

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	18/08/15	vii

PERKARA 11 - PEMATUHAN	74
1101 Pematuhan dan Keperluan Perundangan	74
110101 Pematuhan Dasar	74
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	74
110103 Pematuhan Keperluan Audit	74
110104 Keperluan Perundangan	75
110105 Pelanggaran Dasar	76
GLOSARI	77
Lampiran 1	81
Lampiran 2	82

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	18/08/15	viii

PENGENALAN

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

OBJEKTIF

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

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

Manakala, objektif utama Keselamatan ICT MPSEPANG ialah seperti berikut:

- a. Memastikan kelancaran operasi MPSEPANG dan meminimumkan kerosakan atau 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.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	1

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 menyediakan 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 MPSEPANG 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:

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	2

- a. Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
- b. Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
- c. Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
- d. Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan
- e. Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Aset ICT MPSEPANG terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT MPSEPANG 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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	3

mbolehkan 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 MPSEPANG ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, 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 MPSEPANG. 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 MPSEPANG;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	4

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 MPSEPANG. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod MPSEPANG, 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 MPSEPANG 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 pelanggaran langkah-langkah keselamatan.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	5

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT MPSEPANG dan perlu dipatuhi adalah seperti berikut:

1. Akses atas dasar perlu mengetahui

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

2. Hak akses minimum

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

3. 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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	6

MPSepang 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.

4. Pengasingan

Tugas mewujudkan, 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;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	7

5. 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*;

6. Pematuhan

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	8

6. 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

8. Saling Bergantungan

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	9

PERKARA 01
PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT

Objektif:

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

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini adalah tanggungjawab Yang Dipertua MPSepang dengan dibantu oleh Pasukan Pengurus Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan Ketua Jabatan/Bahagian/Unit.

Yang Dipertua,
Ketua Jabatan/
Bahagian/ Unit
MPSEPANG

010102 Penyebaran Dasar

Dasar ini perlu disebar kepada semua pengguna MPSEPANG (termasuk kakitangan, pembekal, pakar runding dan lain-lain).

ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	10

010103 Penyelenggaraan Dasar	
<p>Dasar Keselamatan ICT MPSEPANG 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.</p> <p>Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT MPSEPANG:</p> <ol style="list-style-type: none"> 1. Kenal pasti dan tentukan perubahan yang diperlukan; 2. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), MPSEPANG; 3. Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JKICT; dan 4. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa. 	ICTSO
010104 Pengecualian Dasar	
Dasar Keselamatan ICT MPSEPANG adalah terpakai kepada semua pengguna ICT MPSEPANG dan tiada pengecualian diberikan.	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	11

PERKARA 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 MPSEPANG.

020101 Yang Dipertua MPSEPANG

Yang Dipertua MPSEPANG adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut:

1. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MPSEPANG;
2. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MPSEPANG;
3. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi;
4. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar

Yang Dipertua
MPSEPANG

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	12

<p>Keselamatan ICT MPSEPANG; dan</p> <p>5. Mempengerusikan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), MPSEPANG.</p>	
<p>020102 Ketua Pegawai Maklumat (CIO)</p>	
<p>Ketua Pegawai Maklumat (CIO) bagi MPSEPANG ialah Timbalan Yang Dipertua MPSEPANG.</p> <p>Peranan dan tanggungjawab CIO adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Membantu Yang Dipertua dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; 2. Menentukan keperluan keselamatan ICT; 3. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT MPSEPANG serta pengurusan risiko dan pengauditan; dan 4. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPSEPANG. 	<p>CIO</p>
<p>020103 Pegawai Keselamatan ICT (ICTSO)</p>	
<p>Pegawai Keselamatan ICT (ICTSO) bagi MPSEPANG ialah Ketua Unit Teknologi Maklumat, MPSEPANG.</p>	<p>ICTSO</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	13

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

1. Mengurus keseluruhan program-program keselamatan ICT MPSEPANG;
2. Menguatkuasakan pelaksanaan Dasar Keselamatan ICT MPSEPANG;
3. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MPSEPANG kepada semua pengguna;
4. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPSEPANG;
5. Menjalankan pengurusan risiko;
6. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPSEPANG berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
7. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
8. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT Kerajaan (GCERT), MPSEPANG dan memaklukkannya kepada CIO;
9. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan
10. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	14

020104 Pengurus ICT

Pengurus ICT bagi MPSEPANG ialah Ketua Unit Teknologi Maklumat, MPSEPANG.

Pengurus ICT

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

1. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPSEPANG;
2. Menentukan kawalan akses pengguna terhadap aset ICT MPSEPANG;
3. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan
4. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPSEPANG.

020105 Pentadbir Sistem ICT

Pentadbir Sistem ICT bagi MPSEPANG ialah Penolong Pengarah Unit Teknologi Maklumat, MPSEPANG.

Pentadbir Sistem ICT

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:

1. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam PERKARA tugas;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	15

<ol style="list-style-type: none"> 2. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MPSEPANG; 3. Memantau aktiviti capaian harian sistem aplikasi pengguna; 4. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan serta merta; 5. Menganalisis dan menyimpan rekod jejak audit; 6. Menyediakan laporan mengenai aktiviti capaian secara berkala; dan 7. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik. 	
---	--

020106 Pengguna

<p>Pengguna mempunyai peranan dan tanggungjawab seperti berikut:</p> <ol style="list-style-type: none"> 1. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPSEPANG; 2. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; 3. Lulus tapisan keselamatan; 	Pengguna
---	----------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	16

<p>4. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MPSEPANG dan menjaga kerahsiaan maklumat MPSEPANG;</p> <p>5. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;</p> <p>6. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan</p> <p>7. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPSEPANG sebagaimana Lampiran 1.</p>	
<p>020107 Jawatan Kuasa Keselamatan ICT MPSEPANG</p>	
<p>Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MPSEPANG.</p> <p>Di MPSEPANG, Mesyuarat Pengurusan Kanan MPSEPANG juga berperanan sebagai JKICT MPSEPANG. Keanggotaan JKICT MPSEPANG adalah seperti berikut:</p> <p>Pengerusi : Yang Dipertua MPSEPANG</p> <p>Ahli : 1. CIO MPSEPANG 2. Timbalan Yang Dipertua 3. Semua Pengarah Jabatan / Ketua Bahagian / Ketua Unit</p>	<p>JKICT MPSEPANG</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	17

4. ICTSO MPSEPANG

Urus Setia bagi JKICT MPSEPANG ialah Unit Teknologi Maklumat.

PERKARA kuasa:

1. Memperakukan/meluluskan dokumen DKICT MPSEPANG;
2. Memantau tahap pematuhan keselamatan ICT;
3. Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MPSEPANG yang mematuhi keperluan DKICT MPSEPANG;
4. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;
5. Memastikan DKICT MPSEPANG selaras dengan dasar-dasar ICT kerajaan semasa;
6. Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa;
7. Membincang tindakan yang melibatkan pelanggaran DKICT MPSEPANG; dan
8. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	18

020108 Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT)

Keanggotaan GCERT adalah seperti berikut:

Pengurus : Ketua Unit Teknologi Maklumat MPSepang

Ahli :

1. Pegawai Teknologi Maklumat di Seksyen Rangkaian dan Perkakasa MPSepang
2. Penolong Pegawai Teknologi Maklumat di Seksyen Rangkaian dan Perkakasa MPSepang

Peranan dan tanggungjawab GCERT adalah seperti berikut:

1. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden;
2. Merekod dan menjalankan siasatan awal insiden yang diterima;
3. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;
4. Menasihati MPSE Pang mengambil tindakan pemulihan dan pengukuhan;
5. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada MPSE Pang; dan

GCERT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSE Pang	VERSI 2.1	10/12/15	19

<p>6. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.</p>	
<p>0202 Pihak Ketiga</p>	
<p>Objektif:</p> <p>Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).</p>	
<p>020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga</p>	
<p>Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal.</p> <p>Perkara yang perlu dipatuhi termasuk yang berikut:</p> <ul style="list-style-type: none"> a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPSEPANG; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; 	<p>CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	20

<ul style="list-style-type: none"> d. Akses kepada aset ICT MPSEPANG perlu berlandaskan kepada perjanjian kontrak; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. <ul style="list-style-type: none"> i. Dasar Keselamatan ICT MPSEPANG; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. f. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPSEPANG sebagaimana Lampiran 1. 	
--	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	21

PERKARA 04
KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan MPSEPANG, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga MPSEPANG 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 MPSEPANG serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
- b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPSEPANG serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan
- c. Mematuhi semua terma dan syarat perkhidmatan yang

Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	22

<p>ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.</p>	
<p>040102 Dalam Perkhidmatan</p>	
<p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:</p> <ol style="list-style-type: none"> a. Memastikan pegawai dan kakitangan MPSEPANG serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MPSEPANG; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPSEPANG 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 MPSEPANG serta pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan oleh MPSEPANG; dan d. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan dan Sumber Manusia, MPSEPANG. 	<p>Semua</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	23

040103 Bertukar Atau Tamat Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- a. Memastikan semua aset ICT dikembalikan kepada MPSEPANG 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 MPSEPANG dan/atau terma perkhidmatan.

Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	24

PERKARA 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. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
- b. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
- c. Memasang alat penggera atau kamera;

Pejabat Ketua
Pegawai
Keselamatan
Kerajaan
(KPKK), CIO
dan ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	25

<ul style="list-style-type: none"> d. Mengehadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan; h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; j. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya. 	
<p>050102 Kawalan Masuk Fizikal</p>	
<p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:</p> <ul style="list-style-type: none"> a. Setiap pengguna MPSEPANG hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan balik kepada MPSEPANG apabila pengguna berhenti atau bersara; 	<p>Semua</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	26

<p>c. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama Kompleks Jabatan Perdana Menteri. Amalan ini juga perlu dipatuhi di kompleks pejabat utama MPSEPANG Sabah dan Sarawak. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan</p> <p>d. Kehilangan pas mestilah dilaporkan dengan segera.</p>	
<p>050103 Kawasan Larangan</p>	
<p>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.</p> <p>Kawasan larangan di MPSEPANG adalah bilik Yang Dipertua, bilik Timbalan Yang Dipertua, pejabat Seksyen Pemantauan Siber (PRISMA), bilik server, bilik Operasi GOE-EGDMS dan Pusat Data (<i>Data Centre</i>) SSO.</p> <p>a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan</p> <p>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.</p>	<p>Pentadbir Sistem</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	27

0502 Keselamatan Peralatan

Objektif:

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

050201 Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;
2. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;
3. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;
4. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;
5. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;
6. 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;

Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	28

7. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;
8. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;
9. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);
10. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;
11. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;
12. Peralatan ICT yang hendak dibawa keluar dari premis MPSEPANG, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;
13. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;
14. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;
15. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;
16. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	29

<p>Pentadbir Sistem ICT untuk di baik pulih;</p> <p>17. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;</p> <p>18. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;</p> <p>19. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (<i>administrator password</i>) yang telah ditetapkan oleh Pentadbir Sistem ICT;</p> <p>20. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;</p> <p>21. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “<i>OFF</i>” apabila meninggalkan pejabat;</p> <p>22. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan</p> <p>23. Memastikan plag dicabut daripada suis utama (<i>main switch</i>) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.</p>	
<p>050202 Media Storan</p>	
<p>Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, <i>optical disk</i>, <i>flash disk</i>, CDROM, <i>thumb drive</i> dan media</p>	<p>Semua</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	30

storan lain.

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
2. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;
3. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
4. 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;
5. Akses dan pergerakan media storan hendaklah direkodkan;
6. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal;
7. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;
8. Semua media storan data yang hendak dilupuskan mestilah

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	31

<p>dihapuskan dengan teratur dan selamat; dan</p> <p>9. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.</p>	
<p>050203 Media Tandatangan Digital</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; 2. Media ini tidak boleh dipindah milik atau dipinjamkan; dan 3. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya. 	<p>Semua</p>
<p>050204 Media Perisian dan Aplikasi</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MPSEPANG; 2. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; 3. Lesen perisian (<i>registration code, serials, CD-keys</i>) perlu disimpan berasingan daripada <i>CD-rom, disk</i> atau media 	<p>Semua</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	32

<p>berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan</p> <p>4. <i>Source code</i> sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.</p>	
--	--

050205 Penyelenggaraan Perkakasan

<p>Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; 2. Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; 3. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; 4. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; 5. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan 6. Semua penyelenggaraan mestilah mendapat kebenaran 	<p>Pegawai Aset dan Seksyen Teknologi Maklumat, MPSEPANG</p>
--	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	33

daripada Pengurus ICT.	
050206 Peralatan di Luar Premis	
<p>Perkakasan yang dibawa keluar dari premis MPSEPANG adalah terdedah kepada pelbagai risiko.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan 2. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. 	Semua
050207 Pelupusan Perkakasan	
<p>Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MPSEPANG dan ditempatkan di MPSEPANG.</p> <p>Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPSEPANG.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui <i>shredding, grinding, degauzing</i> atau pembakaran; 2. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah 	Semua, Pegawai Aset dan Seksyen Teknologi Maklumat, MPSEPANG

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	34

<p>membuat penduaan;</p> <p>3. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;</p> <p>4. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;</p> <p>5. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;</p> <p>6. Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori MyAsset;</p> <p>7. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan</p> <p>8. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:</p> <p>i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, <i>hardisk</i>, <i>motherboard</i> dan sebagainya;</p> <p>ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MPSEPANG;</p>	
---	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	35

<ul style="list-style-type: none"> iii. Memindah keluar dari MPSEPANG mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MPSEPANG; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau <i>thumb drive</i> sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. 	
--	--

0503 Keselamatan Persekitaran

Objektif:

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

050301 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK).

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

1. Merancang dan menyediakan pelan keseluruhan susun atur

Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	36

<p>pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;</p> <ol style="list-style-type: none"> 2. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; 3. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; 4. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; 5. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; 6. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; 7. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan 8. Akses kepada saluran <i>riser</i> hendaklah sentiasa dikunci. 	
<p>050302 Bekalan Kuasa</p>	
<p>Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan</p>	<p>Seksyen Teknologi</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	37

<p>kepada peralatan ICT.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; 2. Peralatan sokongan seperti <i>Uninterruptable Power Supply</i> (UPS) dan penjana (<i>generator</i>) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan 3. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual. 	<p>Maklumat, MPSEPANG dan ICTSO</p>
--	---

050303 Kabel

<p>Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah.</p> <p>Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; 2. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; 3. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan <i>wire tapping</i>; dan 	<p>Seksyen Teknologi Maklumat, MPSEPANG dan ICTSO</p>
--	---

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	38

<p>4. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui <i>trunking</i> bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.</p>	
<p>050304 Prosedur Kecemasan</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MPSEPANG 2004; dan 2. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras. 	<p>Semua dan Pegawai Keselamatan Jabatan</p>
<p>0504 Keselamatan Dokumen</p>	
<p>Objektif:</p> <p>Melindungi maklumat MPSEPANG dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaiian.</p>	
<p>050401 Dokumen</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Setiap dokumen hendaklah difail dan dilabelkan mengikut 	<p>Semua</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	39

<p>klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;</p> <ol style="list-style-type: none"> 2. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; 3. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; 4. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan 5. Menggunakan enkripsi (<i>encryption</i>) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. 	
---	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	40

PERKARA 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:

1. Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal;
2. 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
3. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	41

060102 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;
2. 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;
3. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
4. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	42

060103 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
2. Tugas mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperinci atau di manipulasi; dan
3. 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.

Pengurus ICT
dan ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	43

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:

1. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;
2. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan
3. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

Semua

0603 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

060301 Perancangan Kapasiti

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	44

<p>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.</p> <p>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.</p>	<p>Pentadbir Sistem ICT dan ICTSO</p>
<p>060302 Penerimaan Sistem</p>	
<p>Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.</p>	<p>Pentadbir Sistem ICT dan ICTSO</p>
<p>0604 Perisian Berbahaya</p>	
<p>Objektif:</p> <p>Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, <i>trojan</i> dan sebagainya.</p>	
<p>060401 Perlindungan dari Perisian Berbahaya</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, <i>Intrusion Detection System (IDS)</i> dan <i>Intrusion Prevention System (IPS)</i> serta mengikut 	<p>Semua</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	45

<p>prosedur penggunaan yang betul dan selamat;</p> <ol style="list-style-type: none"> 2. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; 3. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; 4. Mengemas kini anti virus dengan <i>pattern</i> antivirus yang terkini; 5. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; 6. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; 7. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; 8. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan 9. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus. 	
<p>060402 Perlindungan dari <i>Mobile Code</i></p>	
<p>Penggunaan <i>mobile code</i> yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.</p>	<p>Semua</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	46

0605 *Housekeeping*

Objektif:

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

060501 *Backup*

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
2. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat;
3. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;
4. Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan
5. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.

Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	47

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:

1. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;
2. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;
3. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
4. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;
5. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselua oleh Pentadbir Sistem ICT;
6. Semua trafik keluar dan masuk hendaklah melalui *firewall* di

Seksyen
Teknologi
Maklumat,
MPSEPANG

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	48

<p>bawah kawalan MPSEPANG;</p> <p>7. Semua perisian <i>sniffer</i> atau <i>network analyser</i> adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;</p> <p>8. Memasang perisian <i>Intrusion Prevention System (IPS)</i> bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MPSEPANG;</p> <p>9. Memasang <i>Web Content Filtering</i> pada <i>Internet Gateway</i> untuk menyekat aktiviti yang dilarang;</p> <p>10. Sebarang penyambungan rangkaian yang bukan di bawah kawalan MPSEPANG adalah tidak dibenarkan;</p> <p>11. Semua pengguna hanya dibenarkan menggunakan rangkaian MPSEPANG sahaja dan penggunaan modem adalah dilarang sama sekali; dan</p> <p>12. Kemudahan bagi <i>wireless LAN</i> perlu dipastikan kawalan keselamatan.</p>	
---	--

0607 Pengurusan Media

Objektif:

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	49

060701 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua
060702 Prosedur Pengendalian Media	
<p>Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; 2. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; 3. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; 4. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; 5. Menyimpan semua media di tempat yang selamat; dan 6. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat. 	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	50

060703 Keselamatan Sistem Dokumentasi

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

1. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;
2. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan
3. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.

Semua

0608 Pengurusan Pertukaran Maklumat**Objektif:**

Memastikan keselamatan pertukaran maklumat dan perisian antara MPSEPANG 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;
- b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MPSEPANG dengan agensi luar;

Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	51

<p>c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MPSEPANG; dan</p> <p>d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.</p>	
---	--

060802 Pengurusan Mel Elektronik (E-mel)

<p>Penggunaan e-mel di MPSEPANG 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 “<i>Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan</i>” dan mana-mana undang-undang bertulis yang berkuat kuasa.</p> <p>Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Setiap daripada kakitangan MPSepang mempunyai e-mel rasmi masing-masing yang digunakan bagi tujuan rasmi; 2. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MPSEPANG sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; 3. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MPSEPANG; 4. Memastikan subjek dan kandungan e-mel adalah berkaitan dan 	<p>Semua</p>
--	--------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	52

<p>menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;</p> <ol style="list-style-type: none"> 5. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; 6. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; 7. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; 8. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; 9. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; 10. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; 11. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; 12. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; 13. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan 	
---	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	53

<p>sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan</p> <p>14. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.</p>	
--	--

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

<p>Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; 2. Maklumat yang terlibat dalam transaksi dalam talian (<i>on-line</i>) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan 3. Integriti maklumat yang disediakan untuk sistem yang boleh 	<p>Semua</p>
---	--------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	54

dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
060902 Maklumat Umum	
<p>Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; 2. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan 3. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web. 	Semua
0610 Pemantauan	
<p>Objektif:</p> <p>Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.</p>	
061001 Pengauditan dan Forensik ICT	
<p>ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut:</p> <ol style="list-style-type: none"> 1. Sebarang percubaan pencerobohan kepada sistem ICT 	ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	55

<p>MPSEPANG;</p> <ol style="list-style-type: none"> 2. Serangan kod perosak (<i>malicious code</i>), halangan pemberian perkhidmatan (<i>denial of service</i>), <i>spam</i>, pemalsuan (<i>forgery</i>, <i>phising</i>), pencerobohan (<i>intrusion</i>), ancaman (<i>threats</i>) dan kehilangan fizikal (<i>physical loss</i>); 3. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; 4. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; 5. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; 6. Aktiviti instalasi dan penggunaan perisian yang membebaskan jalur lebar (<i>bandwidth</i>) rangkaian; 7. Aktiviti penyalahgunaan akaun e-mel; dan 8. Aktiviti penukaran alamat IP (<i>IP address</i>) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT. 	
<p>061002 Jejak Audit</p>	
<p>Setiap sistem mestilah mempunyai jejak audit (<i>audit trail</i>). 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.</p> <p>Jejak audit hendaklah mengandungi maklumat-maklumat berikut:</p>	<p>Pentadbir Sistem ICT</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	56

1. Rekod setiap aktiviti transaksi;
2. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;
3. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
4. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara.

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	57

061003 Sistem Log

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

1. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
2. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan
3. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.

Pentadbir
Sistem ICT

061004 Pemantauan Log

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;
2. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;
3. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;
4. Aktiviti pentadbiran dan operator sistem perlu direkodkan;

Seksyen
Teknologi
Maklumat,
MPSEPANG
dan Pentadbir
Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	58

<p>5. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan</p> <p>6. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MPSEPANG atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.</p>	
--	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	59

**PERKARA 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:

1. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;
2. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
3. Keselamatan maklumat yang dicapai menggunakan kemudahan

Seksyen
Teknologi
Maklumat,
MPSEPANG
dan ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	60

<p>atau peralatan mudah alih; dan</p> <p>4. Kawalan ke atas kemudahan pemrosesan maklumat.</p>	
<p>0702 Pengurusan Capaian Pengguna</p>	
<p>Objektif:</p> <p>Mengawal capaian pengguna ke atas aset ICT MPSEPANG.</p>	
<p>070201 Akaun Pengguna</p>	
<p>Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:</p> <ol style="list-style-type: none"> 1. Akaun yang diperuntukkan oleh MPSEPANG sahaja boleh digunakan; 2. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; 3. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; 4. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MPSEPANG. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; 	<p>Semua dan Pentadbir Sistem ICT</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	61

<p>5. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan</p> <p>6. Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:</p> <ul style="list-style-type: none"> i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar PERKARA tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan. 	
070202 Hak Capaian	
<p>Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.</p>	<p>Pentadbir Sistem ICT</p>
070203 Pengurusan Kata Laluan	
<p>Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MPSEPANG seperti berikut:</p> <ul style="list-style-type: none"> 1. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; 	<p>Semua dan Pentadbir Sistem ICT</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	62

<ol style="list-style-type: none"> 2. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; 3. Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus; 4. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; 5. Kata laluan <i>windows</i> dan <i>screen saver</i> hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; 6. Kata laluan hendaklah tidak dipaparkan semasa <i>input</i>, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; 7. Kuatkuasakan pertukaran kata laluan semasa <i>login</i> kali pertama atau selepas <i>login</i> kali pertama atau selepas kata laluan diset semula; 8. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; 9. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; 10. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan 11. Mengelakkan penggunaan semula kata laluan yang baru digunakan. 	
---	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	63

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 atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;
2. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan
3. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.

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

Pentadbir
Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	64

<p>dengan:</p> <ol style="list-style-type: none"> 1. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MPSEPANG, rangkaian agensi lain dan rangkaian awam; 2. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan 3. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT. 	<p>dan ICTSO</p>
<p>070302 Capaian Internet</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Penggunaan Internet di MPSEPANG hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan <i>malicious code</i>, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MPSEPANG; 2. Kaedah <i>Content Filtering</i> mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; 3. Penggunaan teknologi (<i>packet shaper</i>) untuk mengawal aktiviti (<i>video conferencing, video streaming, chat, downloading</i>) adalah perlu bagi menguruskan penggunaan jalur lebar (<i>bandwidth</i>) yang 	<p>Pentadbir Rangkaian</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	65

<p>maksimum dan lebih berkesan;</p> <ol style="list-style-type: none"> 4. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; 5. Laman yang dilayari hendaklah hanya yang berkaitan dengan PERKARA kerja dan terhad untuk tujuan yang dibenarkan oleh Yang Dipertua/ pegawai yang diberi kuasa; 6. Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; 7. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet; 8. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; 9. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MPSEPANG; 10. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti <i>newsgroup</i> dan <i>bulletin board</i>. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; 11. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan 12. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti 	<p>Pengurus ICT</p> <p>Semua</p>
--	----------------------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	66

<p>berikut:</p> <ol style="list-style-type: none"> i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah. 	
<p>0704 Kawalan Capaian Sistem Pengoperasian</p>	
<p>Objektif:</p> <p>Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.</p>	
<p>070401 Capaian Sistem Pengoperasian</p>	
<p>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:</p> <ol style="list-style-type: none"> 1. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan 2. Merekodkan capaian yang berjaya dan gagal. 	<p>Pentadbir Sistem ICT dan ICTSO</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	67

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

1. Mengesahkan pengguna yang dibenarkan;
2. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan
3. Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

1. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;
2. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;
3. Mengehadkan dan mengawal penggunaan program; dan
4. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

070402 Kad Pintar

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	68

<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; 2. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; 3. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan 4. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Seksyen Teknologi Maklumat, Bahagian Khidmat Pengurusan dan Sumber Manusia, MPSEPANG. 	<p>Semua</p>
---	--------------

0705 Kawalan Capaian Aplikasi dan Maklumat

Objektif:

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	69

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:

1. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;
2. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);
3. Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;
4. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan
5. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.

Pentadbir
Sistem ICT
dan ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	70

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: 1. 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: 1. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	71

PERKARA 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:

1. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;
2. 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;
3. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat

Pemilik Sistem,
 Pentadbir Sistem ICT dan ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	72

<p>kesilapan pemprosesan atau perlakuan yang disengajakan; dan</p> <p>4. 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.</p>	
080102 Pengesahan Data Input dan Output	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 1. Data <i>input</i> bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan 2. Data <i>output</i> daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat. 	<p>Pemilik Sistem dan Pentadbir Sistem ICT</p>
0802 Kawalan Kriptografi	
<p>Objektif:</p> <p>Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.</p>	
080201 Enkripsi	
<p>Pengguna hendaklah membuat enkripsi (<i>encryption</i>) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.</p>	<p>Semua</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	73

080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
080203 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.	Semua
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: <ol style="list-style-type: none"> 1. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; 2. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; 	Pemilik Sistem dan Pentadbir Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	74

<ol style="list-style-type: none"> 3. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; 4. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan 5. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan. 	
--	--

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;

Pemilik Sistem dan Pentadbir Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	75

<p>c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;</p> <p>d. Akses kepada kod sumber (<i>source code</i>) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan</p> <p>e. Menghalang sebarang peluang untuk membocorkan maklumat.</p>	
<p>080402 Pembangunan Perisian Secara <i>Outsource</i></p>	
<p>Pembangunan perisian secara <i>outsource</i> perlu diselia dan dipantau oleh pemilik sistem.</p> <p>Kod sumber (<i>source code</i>) bagi semua aplikasi dan perisian adalah menjadi hak milik MPSEPANG.</p>	<p>Seksyen Teknologi Maklumat dan Pentadbir Sistem ICT</p>
<p>0805 Kawalan Teknikal Keterdedahan (<i>Vulnerability</i>)</p>	
<p>Objektif:</p> <p>Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.</p>	
<p>080501 Kawalan dari Ancaman Teknikal</p>	
<p>Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.</p>	<p>Pentadbir Sistem ICT</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	76

Perkara yang perlu dipatuhi adalah seperti berikut:

1. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;
2. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan
3. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	77

PERKARA 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.

090101 Mekanisme Pelaporan

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 GCERT MPSEPANG dengan kadar segera:

1. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
2. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	78

3. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
4. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
5. Berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak dijangka.

Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di MPSEPANG sepertimana **Lampiran 2**.

Prosedur pelaporan insiden keselamatan ICT berdasarkan:

1. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan
2. 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.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	79

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 MPSEPANG.

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:

1. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;
2. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
3. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;
4. Menyediakan tindakan pemulihan segera; dan
5. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	80

PERKARA 10
Pengurusan Kesenambungan Perkhidmatan

1001 Dasar Kesenambungan Perkhidmatan

Objektif:

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

100101 Pelan Kesenambungan Perkhidmatan

Pelan Kesenambungan Perkhidmatan (*Business Continuity Management - BCM*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesenambungan perkhidmatan.

Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKICT MPSEPANG. Perkara-perkara berikut perlu diberi perhatian:

1. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
2. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;
3. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau

Pengurus ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	81

dalam jangka masa yang telah ditetapkan;

4. Mendokumentasikan proses dan prosedur yang telah dipersetujui;
5. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
6. Membuat *backup*; dan
7. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

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

1. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
2. Senarai personel MPSEPANG dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden;
3. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
4. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
5. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	82

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.

MPSEPANG hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

PERKARA 11 PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif:

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	83

110101 Pematuhan Dasar	
<p>Setiap pengguna di MPSEPANG hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MPSEPANG dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.</p> <p>Semua aset ICT di MPSEPANG termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Yang Dipertua/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.</p> <p>Sebarang penggunaan aset ICT MPSEPANG selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MPSEPANG.</p>	Semua
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
<p>ICTSO hendaklah memastikan semua prosedur keselamatan dalam PERKARA tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.</p> <p>Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.</p>	ICTSO
110103 Pematuhan Keperluan Audit	
<p>Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke</p>	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	84

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.	
---	--

110104 Keperluan Perundangan

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

Semua

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 Pentadbiran 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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	85

<p>Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (<i>Wireless Local Area Network</i>) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;</p> <p>9. Surat Arahan Yang Dipertua MPSEPANG - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;</p> <p>10. Surat Arahan Yang Dipertua MPSEPANG - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;</p> <p>11. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);</p> <p>12. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;</p> <p>13. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;</p> <p>14. Akta Tandatangan Digital 1997;</p> <p>15. Akta Rahsia Rasmi 1972;</p> <p>16. Akta Jenayah Komputer 1997;</p> <p>17. Akta Hak Cipta (Pindaan) Tahun 1997;</p> <p>18. Akta Komunikasi dan Multimedia 1998;</p> <p>19. Perintah-Perintah Am;</p> <p>20. Arahan Perbendaharaan;</p>	
--	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	86

<p>21. Arahan Teknologi Maklumat 2007;</p> <p>22. Garis Panduan Keselamatan MPSEPANG 2004; dan</p> <p>23. <i>Standard Operating Procedure</i> (SOP) ICT MPSEPANG.</p>	
<p>110105 Pelanggaran Dasar</p>	
<p>Pelanggaran Dasar Keselamatan ICT MPSEPANG boleh dikenakan tindakan tatatertib.</p>	<p>Semua</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	87

GLOSARI	
<i>Antivirus</i>	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, <i>optical disk</i> , <i>flash disk</i> , CDROM, <i>thumb drive</i> untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
<i>Backup</i>	Proses penduaan sesuatu dokumen atau maklumat.
<i>Bandwidth</i>	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	<i>Chief Information Officer</i> Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
<i>Denial of service</i>	Halangan pemberian perkhidmatan.
<i>Downloading</i>	Aktiviti muat-turun sesuatu perisian.
<i>Encryption</i>	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	88

GLOSARI	
<i>Firewall</i>	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.
<i>Forgery</i>	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (<i>information theft/espionage</i>), penipuan (<i>hoaxes</i>).
GCERT	<i>Government Computer Emergency Response Team</i> atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
<i>Hard disk</i>	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
<i>Hub</i>	Hab (<i>hub</i>) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bus berbentuk bintang dan menyiarkan (<i>broadcast</i>) data yang diterima daripada sesuatu <i>port</i> kepada semua <i>port</i> yang lain.
ICT	<i>Information and Communication Technology</i> (Teknologi Maklumat dan Komunikasi).

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	89

GLOSARI	
ICTSO	<p><i>ICT Security Officer</i></p> <p>Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.</p>
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (<i>server</i>) atau komputer lain.
<i>Internet Gateway</i>	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
<i>Intrusion Detection System (IDS)</i>	<p>Sistem Pengesanan Pencerobohan</p> <p>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 <i>host</i> atau rangkaian.</p>
<i>Intrusion Prevention System (IPS)</i>	<p>Sistem Pencegah Pencerobohan</p> <p>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 <i>malicious code</i>.</p> <p>Contohnya: <i>Network-based IPS</i> yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.</p>

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	90

GLOSARI	
LAN	<i>Local Area Network</i> Rangkaian Kawasan Setempat yang menghubungkan komputer.
<i>Logout</i>	<i>Log-out</i> komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
<i>Malicious Code</i>	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, <i>trojan horse</i> , <i>worm</i> , <i>spyware</i> 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.
<i>Outsource</i>	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 <i>spreadsheet</i> dan <i>word processing</i> ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
<i>Public-Key Infrastructure</i>	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	91

GLOSARI	
<i>(PKI)</i>	melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
<i>Router</i>	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
<i>Screen Saver</i>	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
<i>Server</i>	Pelayan komputer
<i>Switches</i>	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian <i>Carrier Sense Multiple Access/Collision Detection</i> (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
<i>Threat</i>	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
<i>Uninterruptible Power Supply (UPS)</i>	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
<i>Video Conference</i>	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	92

GLOSARI	
<i>Video Streaming</i>	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.
<i>Wireless LAN</i>	Jaringan komputer yang terhubung tanpa melalui kabel.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	93

Lampiran 1

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MPSEPANG

Nama (Huruf Besar) :

No. Kad Pengenalan :

Jawatan :

Bahagian :

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	94

Adalah dengan sesungguhnya dan sebenarnya mengaku bahwa :-

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

Tanda :
tangan

Tarikh :

Pengesahan Pegawai Keselamatan ICT

.....

(Nama Pegawai Keselamatan ICT)

b.p. Yang Dipertua MPSEPANG

Tarikh:

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	95

Lampiran 2

Penunjuk :

SOP - Standard Operating Procedure

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPSEPANG	VERSI 2.1	10/12/15	96