LEMBAGA LADA MALAYSIA

DASAR KESELAMATAN ICT (DKICT)

LEMBAGA LADA MALAYSIA

versi 5.0

BAHAGIAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

LEMBAGA LADA MALAYSIA

DASAR KESELAMATAN ICT (DKICT)
LEMBAGA LADA MALAYSIA

versi 5.0

2024

BAHAGIAN TEKNOLOGI MAKLUMAT & KOMUNIKASI
LEMBAGA LADA MALAYSIA

SEJARAH DOKUMEN

Tarikh	Versi	Kelulusan	Tarikh Kuatkuasa
11 Mei 2012	1.0	JPICT Bil. 1/2012	14 Mei 2012
28 Feb 2018	2.0	JPICT Bil. 1/2018	18 April 2018
9 Nov 2020	3.0	JPICT Bil. 3/2020	3 Disember 2020
6 Oktober 2023	4.0	MKSP Bil.2/2023	9 Oktober 2023
31 Julai 2024	5.0	MKSP Bil.1/2024	6 Ogos 2024

ISI KANDUNGAN

PENGENALAN 1

OBJEKTIF 1

PERNYATAAN DASAR 1

SKOP 2

PRINSIP-PRINSIP 5

BIDANG 01 – PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 DASAR KESELAMATAN ICT 8
010101 Pelaksanaan Dasar 8
010102 Penyebaran Dasar 8
010103 Penyelenggaraan Dasar 8
010104 Pengecualian Dasar 8

BIDANG 02 - ORGANISASI KESELAMATAN

0201 ORGANISASI KESELAMATAN MPB 9
020101 Ketua Pengarah (KP) MPB 9
020102 Ketua Pegawai Maklumat (CIO) 9
020103 Pegawai Keselamatan ICT (ICTSO) 10
020104 Pengurus ICT 11
020105 Pentadbir ICT 11
020106 Pekhidmat MPB 12
020107 Jawatankuasa Pemandu ICT MPB (JPICT MPB) 13
020108 Pasukan Tindak Balas Insiden Keselamatan ICT MPB (CERT) 14

0202 PIHAK KETIGA 14
020201 Keperluan Keselamatan ICT di dalam Kontrak dengan Pihak Ketiga 14

BIDANG 03 - PENGURUSAN ASET

0301 TANGGUNGJAWAB TERHADAP ASET 16
030101 Inventori Aset ICT 16
0302 PENGELASAN DAN PENGENDALIAN MAKLUMAT 17
030201 Pengelasan Maklumat 17
030202 Pengendalian Maklumat 17

BIDANG 04 - KESELAMATAN SUMBER MANUSIA

0401 KESELAMATAN SUMBER MANUSIA 18
040101 Sebelum Perkhidmatan 18
040102 Semasa Perkhidmatan 18
040103 Tamat Perkhidmatan atau Pertukaran Perkhidmatan 19

BIDANG 05 - KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 KESELAMATAN KAWASAN 20
050101 Keselamatan Kawasan Fizikal 20
050102 Kawalan Masuk Fizikal 21
050103 Kawasan Larangan ICT 21
050104 Perlindungan Kawasan ICT Dari Ancaman Luar Dan Bencana Alam 21
050105 Kawalan Kawasan Penghantaran Barangan dan Loading Area 22
0502 KESELAMATAN ASET ICT 23
050201 Peralatan dan Perkakasan ICT 23
050202 Media Storan Digital 24
050203 Media Tandatangan Digital 25
050204 Media Perisian dan Aplikasi 26
050205 Utiliti Sokongan 26
050206 Penyelenggaraan Perkakasan 26
050207 Aset ICT di Luar Premis 27
050208 Pelupusan dan Guna Semula Perkakasan 27
0503 KESELAMATAN PERSEKITARAN 29
050301 Kawalan Persekitaran 29
050302 Bekalan Kuasa 30
050303 Kabel 30
050304 Prosedur Kecemasan Kebakaran 31

0504 KESELAMATAN DOKUMEN 31
050401 Dokumen 31

BIDANG 06 – PENGURUSAN OPERASI DAN KOMUNIKASI

0601 PENGURUSAN PROSEDUR OPERASI DAN TANGGUNGJAWAB.....32
060101 Pengendalian Prosedur Operasi ICT 32
060102 Kawalan Perubahan 32
060103 Pengasingan Tugas dan Tanggungjawab 33
0602 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA 34
060201 Perkhidmatan 34
060202 Pemantauan Perkhidmatan Pihak Ketiga 34
0603 PERANCANGAN DAN PENERIMAAN SISTEM 35
060301 Pengurusan Kapasiti..... 35
060302 Perancangan Kapasiti..... 35
060303 Penerimaan Sistem 35
0604 KAWALAN TERHADAP PERISIAN BERBAHAYA 36
060401 Perlindungan Dari Perisian Berbahaya..... 36
060402 Kawalan terhadap kod berbahaya (Malicious Code) . 36
060403 Kawalan terhadap Mobile Code..... 36
0605 HOUSEKEEPING (BACK UP) 37
060501 Back-up 37
0606 PENGURUSAN KESELAMATAN RANGKAIAN 38
060601 Kawalan Infrastruktur Rangkaian..... 38
0607 PENGENDALIAN MEDIA.....39
060701 Penghantaran dan Pemindahan 39
060702 Prosedur Pengendalian Dan Pelupusan Media 39
060703 Keselamatan Sistem Dokumentasi..... 40
0608 PENGURUSAN PERTUKARAN MAKLUMAT.....41
060801 Pertukaran Maklumat..... 41
060802 Pengurusan Mel Elektronik (E-mel) 42
060803 Business Information System.....42
060804 Kawalan Media Sosial.....42
0609 PERKHIDMATAN TRANSAKSI ATAS TALIAN 43
060901 Transaksi atas Talian..... 43
060902 Maklumat Capaian Umum 43
0610 PEMANTAUAN 44
061001 Pengauditan dan Forensik ICT 44
061002 Jejak Audit 44
061003 Sistem Log..... 45
061004 Pemantauan Log 45
061005 Perlindungan Log..... 46
061006 Log untuk Pentadbir Sistem..... 46
061007 Log Kerosakan 46
061008 Penyeragaman Waktu 46

BIDANG 07 - KAWALAN CAPAIAN

0701 KAWALAN CAPAIAN 47
070101 Keperluan Kawalan Capaian 47
0702 PENGURUSAN CAPAIAN PENGGUNA 48
070201 Pendaftaran Akaun Pengguna..... 48
070202 Hak Capaian (privilege) 49
070203 Semakan Hak Capaian Pengguna 49
070204 Pengurusan Kata Laluan Pengguna..... 49
0703 TANGGUNGJAWAB PENGGUNA.....50
070301 Penggunaan Akaun dan Kata Laluan 50
070302 Unattended User Equipment 51
070303 Clear Desk dan Clear Screen..... 51
070304 Penggunaan Komputer/Notebook 52
0704 KAWALAN CAPAIAN RANGKAIAN.....53
070401 Capaian Rangkaian 53
070402 Capaian Internet..... 53
070403 Peralatan Dalam Rangkaian..... 55
070404 Capaian ke atas Port Untuk Tujuan Diagnostik 55

070405 Pengasingan Dalam Rangkaian 55
070406 Kawalan Penghalaan (Routing) Rangkaian..... 56
0705 KAWALAN CAPAIAN SISTEM PENGOPERASIAN 57
070501 Capaian Sistem Pengoperasian 57
070502 Secure Log-on..... 57
070503 Pengenalan dan Pengesahan pengguna..... 58
070504 Penggunaan Sistem Utiliti..... 58
070505 Session Time-Out..... 58
070506 Had Masa Capaian..... 58
0706 KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT 59
070601 Capaian Aplikasi dan Maklumat 59
070602 Larangan Capaian Maklumat..... 59
070603 Pengasingan Sistem Kritikal..... 59
0707 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH 60
070701 Peralatan Mudah Alih 60
070702 Kemudahan Kerja Jarak Jauh 60

BIDANG 08 - PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 KESELAMATAN DALAM MEMBANGUNKAN SISTEM DAN APLIKASI.....61
080101 Keperluan Keselamatan Sistem Maklumat..... 61
080102 Analisa Dan Spesifikasi Keperluan Keselamatan..... 61
0802 KEBOLEHPERCAYAAN PEMPROSESAN DALAM APLIKASI 62
080201 Pengesahan Data Input..... 62
080202 Kawalan Bagi Pemprosesan Dalaman 62
080203 Integriti Maklumat 62
080204 Pengesahan Data Output..... 62
0803 KAWALAN KRIPTOGRAFI.....63
080301 Enkripsi..... 63
080302 Tandatangan Digital..... 63
080303 Pengurusan Kunci Kriptografi..... 63
0804 KESELAMATAN FAIL SISTEM 64
080401 Kawalan Perisian (Operational Software)..... 64
080402 Kawalan Data Pengujian Sistem..... 64
080403 Kawalan Capaian kepada Kod Sumber (Source Code) 65
0805 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN PROSESAN SOKONGAN 66
080501 Kawalan Perubahan 66
080502 Keperluan Kajian Teknikal Terhadap Aplikasi Selepas Perubahan Sistem Pengoperasian 66
080503 Pembangunan Perisian Secara Outsource..... 67
0806 PENGURUSAN KELEMAHAN TEKNIKAL.....68
080601 Kawalan Kelemahan Teknikal 68
0807 KAWALAN TEKNIKAL KETERDEDAHAN (*VULNERABILITY*).....69
080701 Kawalan dari Ancaman Teknikal 69

BIDANG 09 - PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 MEKANISME PELAPORAN INSIDEN KESELAMATAN ICT.....70
090101 Mekanisme Pelaporan..... 70
090102 Pelaporan Kelemahan Keselamatan 71
0902 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT 72
090201 Maklumat Insiden Keselamatan ICT..... 72
090202 Pembelajaran Dari Insiden Kelemahan Maklumat..... 72
090203 Pengumpulan Bukti..... 73

BIDANG 10 - PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 DASAR KESINAMBUNGAN PERKHIDMATAN.....74
100101 Pelan Kesinambungan Perkhidmatan..... 74

BIDANG 11 – PEMATUHAN

1101 PEMATUHAN DAN KEPERLUAN PERUNDANGAN 76
110101 Pematuhan Dasar..... 76
110102 Pematuhan dengan Dasar dan Keperluan Teknikal .. 76
110103 Pematuhan Keperluan Audit..... 76
110104 Keperluan Perundangan..... 77
110105 Pelanggaran Dasar..... 78

PENGHARGAAN

Setinggi-tinggi penghargaan diucapkan kepada Unit Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) dan Kementerian Perladangan dan Komoditi (KPK) sebagai rujukan untuk membangunkan Dasar Keselamatan ICT (DKICT) Lembaga Lada Malaysia (MPB) ini.

PENGENALAN

Dasar Keselamatan ICT (DKICT) MPB (*Malaysian Pepper Board)* 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 MPB.

OBJEKTIF

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

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

Manakala, objektif utama Keselamatan ICT MPB ialah seperti berikut:

a. Memastikan kelancaran operasi MPB 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 MPB.

PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan.

Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a. Melindungi maklumat rahsia rasmi dan maklumat rasmi MPB 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 MPB merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

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

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

SKOP

Aset ICT terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT MPB menetapkan keperluan-keperluan asas berikut:

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

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

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT MPB ini merangkumi perlindungan semua bentuk maklumat MPB yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan. 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. 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 MPB;

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 visi MPB. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod, 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 bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

f. Premis Komputer Dan Komunikasi

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

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT MPB 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.

2. Hak akses minimum

Hak akses perlu ditentukan dari semasa ke semasa mengikut keperluan berdasarkan kepada peranan dan tanggungjawab pengguna/bidang 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 mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

4. Pengasingan

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi.

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 dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

6. Pematuhan

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

7. 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~~/~~; 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.

BIDANG 01 – PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT

Objektif :

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan fungsi-fungsi utama MPB dan perundangan yang berkaitan.

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah (KP) dan dibantu oleh Timbalan Ketua Pengarah, semua Ketua Bahagian, Pengarah Wilayah dan Ketua Unit serta Pegawai Keselamatan ICT.

Tindakan: KP/TKP/Ketua Bahagian/Pengarah Wilayah/Ketua Unit /ICTSO

010102 Penyebaran Dasar

Dasar ini hendaklah disebarkan dan dipatuhi oleh semua pengguna aset ICT MPB termasuk kontraktor dan pihak ketiga yang berurusan atau memberikan perkhidmatan ICT kepada MPB.

Tindakan: ICTSO

010103 Penyelenggaraan Dasar

Dasar ini boleh disemak dan dipinda jika perlu selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial.

Tindakan: ICTSO

010104 Pengecualian Dasar

Dasar ini adalah terpakai kepada semua kakitangan MPB dan kontraktor/vendor/pihak ketiga.

Tindakan: Semua

BIDANG 02 - ORGANISASI KESELAMATAN

0201 Organisasi Keselamatan MPB

Objektif :

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

020101 Ketua Pengarah (KP) MPB

KP MPB adalah berperanan dan bertanggungjawab dalam perkara-perkara berikut:

a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MPB;
b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MPB;
c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan
d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MPB.

Tindakan: KP

020102 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) bagi MPB adalah Ketua Pengarah atau Timbalan Ketua Pengarah.

Peranan dan tanggungjawab CIO adalah seperti berikut:

a) Membantu KP dalam melaksanakan tugas-tugas yang melibatkan ICT dan keselamatan ICT;
b) Meluluskan semua prosedur, standard, dan garis panduan keselamatan ICT MPB;
c) Meluluskan perlaksanaan atau aktiviti keselamatan ICT MPB;
d) Menentukan keperluan keselamatan ICT;
e) Meluluskan pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT MPB serta pengurusan risiko dan pengauditan; dan
f) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPB.

Tindakan: CIO

020103 Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT (ICTSO) bagi MPB ialah Pegawai Teknologi Maklumat atau Penolong Pegawai Teknologi Maklumat Bahagian Teknologi Maklumat & Komunikasi MPB (TMK).

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

a) Mengurus keseluruhan program-program keselamatan ICT MPB;
b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT MPB;
c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MPB kepada semua pengguna;
d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPB;
e) Menjalankan pengurusan risiko;
f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPB berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
h) Melaporkan insiden keselamatan ICT kepada kepada CIO;
i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;
j) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT;
k) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan
l) Koordinator Pengurusan Kesinambungan Perkhidmatan (Koordinator PKP) MPB.

Tindakan: ICTSO

020104 Pengurus ICT

Pengurus ICT bagi MPB ialah Ketua Bahagian Teknologi Maklumat & Komunikasi MPB (TMK).

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

a) Mengkaji, menguji dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPB;
b) Membuat penilaian keberkesanan kawalan keselamatan ICT;
c) Meluluskan prosedur teknikal perlaksanaan kawalan keselamatan;
d) Menentukan kawalan akses pengguna terhadap aset ICT MPB;
e) Memastikan semua dasar keselamatan ICT di patuhi;
f) Mengambil tindakan terhadap pencerobohan, ancaman atau penemuan mengenai kelemahan keselamatan ICT; dan
g) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPB.

Tindakan: Pengurus ICT

020105 Pentadbir ICT

Pentadbir ICT ialah Penolong Pegawai Teknologi Maklumat (PPTM) atau Juruteknik Komputer yang dilantik untuk mentadbir dan menguruskan sistem, perkakasan dan rangkaian ICT seperti berikut:

a) Pentadbir Rangkaian;
b) Pentadbir Laman Web (Web Master); dan
c) Pentadbir Sistem Aplikasi;

Peranan dan tanggungjawab Pentadbir ICT adalah seperti berikut:

a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MPB;
c) Memantau aktiviti capaian harian sistem aplikasi pengguna;
d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;
e) Menganalisis dan menyimpan rekod jejak audit

f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan
g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.

Tindakan: Pentadbir ICT

020106 Pekhidmat MPB (Pekhidmat)

Pekhidmat MPB adalah pegawai-pegawai yang dilantik oleh MPB secara tetap, kontrak dan sambilan.

Pekhidmat mempunyai peranan dan tanggungjawab seperti berikut:

a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPB;
b) Mengetahui dan memahami implikasi keselamatan ICT, kesan dari tindakannya;
c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;
d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MPB dan menjaga kerahsiaan maklumat MPB;
e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;
f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan
g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPB sebagaimana di Lampiran 1.

Tindakan : Pekhidmat MPB

020106 Jawatankuasa Pemandu ICT MPB (JPICT MPB)

Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa yang bertanggungjawab ke atas segala perancangan, pelaksanaan, pemantauan dan strategi keselamatan ICT MPB. Mesyuarat perlu diadakan sekurang-kurangnya tiga kali setahun dan segala perancangan, pelaksanaan, pemantauan dan strategi keselamatan ICT MPB perlu dijadikan agenda mesyuarat sekurang-kurangnya sekali setahun.

Keanggotaan JPICT MPB adalah seperti berikut:

a) Pengerusi : KP MPB

Ahli :

i. Timbalan Ketua Pengarah
ii. Ketua Pegawai Maklumat (CIO)
iii. Semua Ketua Bahagian
iv. Semua Pengarah Wilayah,
v. Ketua Unit atau wakil
vi. ICTSO

Bidang kuasa berkaitan keselamatan ICT :

a) Memperakui/meluluskan dokumen DKICT MPB;
b) Meluluskan tahap pematuhan keselamatan ICT;
c) Meluluskan teknologi yang bersesuaian untuk dilaksanakan di dalam memperkukuhkan keselamatan ICT;
d) Meluluskan cadangan penyelesaian terhadap keperluan keselamatan ICT;
e) Memastikan DKICT MPB selaras dengan dasar-dasar ICT kerajaan semasa;
f) Meluluskan laporan dan membincangkan hal-hal keselamatan ICT semasa;
g) Meluluskan tindakan yang melibatkan pelanggaran DKICT MPB; dan
h) Meluluskan tindakan yang perlu diambil mengenai sebarang insiden.

Tindakan : JPICT

020107 Pasukan Tindak Balas Insiden Keselamatan ICT MPB (CERT)

Pengguna wajib melaporkan sebarang insiden ICT kepada pasukan tindak balas insiden keselamatan ICT MPB mengikut prosedur yang ditetapkan apabila berlaku insiden yang menjejaskan keselamatan ICT.

Pasukan tindak balas insiden keselamatan ICT MPB adalah pasukan yang akan bertindak semasa berlaku insiden keselamatan di MPB.

Peranan dan tanggungjawab CERT adalah seperti berikut :

a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden;
b) Merekod dan menjalankan siasatan awal insiden yang diterima;
c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;
d) Menasihati CIO mengambil tindakan pemulihan dan pengukuhan;
e) Memberikan khidmat nasihat dan amaran awal insiden; dan
f) Menyebarkan maklumat berkaitan pengukuhan keselamatan ICT kepada pihak yang berkepentingan.

Tindakan : Semua

0202 Pihak Ketiga

Objektif :

Menjamin keselamatan semua aset ICT yang digunakan oleh Pembekal, Kontraktor, Pakar Runding dan lain-lain adalah terkawal keselamatannya dan tidak disalahguna.

020201 Keperluan Keselamatan ICT di dalam Kontrak dengan Pihak Ketiga

Perjanjian kontrak dengan pihak ketiga yang berurusan dengan aset ICT perlu bagi memastikan penggunaan maklumat dan kemudahan prosesan maklumat dikawal.

Perkara yang perlu dipatuhi di dalam perjanjian adalah seperti berikut:

a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPB;
b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;
c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;
d) Akses kepada aset ICT MPB perlu berlandaskan kepada perjanjian kontrak;
e) Memastikan semua syarat-syarat keselamatan dan prosedur dipatuhi dan dinyatakan dengan jelas kepada pihak ketiga;

Tindakan : Semua

BIDANG 03 - PENGURUSAN ASET

0301 Tanggungjawab Terhadap Aset

Objektif :

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MPB.

030101 Inventori Aset ICT

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

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dan dikemas kini;
b) Memastikan maklumat penyelenggaraan aset ICT direkod dan sentiasa dikemas kini;
c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;
d) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MPB;
e) Semua pegerakan dan peminjaman aset ICT direkod dan dipantau;
f) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan;
g) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan
h) Peraturan bagi pengendalian pelupusan aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan.

Tindakan : UPA, TMK dan Semua

0302 Pengelasan dan Pengendalian Maklumat

Objektif :

Memastikan setiap maklumat diberikan tahap perlindungan yang bersesuaian.

030201 Pengelasan Maklumat

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut Akta Rahsia Rasmi.

Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan seperti berikut:

a) Rahsia Besar;
b) Rahsia;
c) Sulit; atau
d) Terhad.

Tindakan : PTA, Ketua Bahagian, Pengarah Wilayah dan Ketua Unit

030202 Pengendalian Maklumat

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

a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan ;
b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
c) Menentukan maklumat sedia untuk digunakan;
d) Menjaga kerahsiaan kata laluan;
e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

Tindakan : PTA, TMK dan Semua

BIDANG 04 - KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia

Objektif :

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

040101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

a) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPB yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan
b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

Tindakan : PSM

040102 Semasa Perkhidmatan

Objektif :

Memastikan semua pekhidmat, kontraktor dan pihak ketiga mempunyai kesedaran terhadap ancaman keselamatan dan sedar akan tanggungjawab bagi memastikan segala dasar keselamatan dilaksanakan di dalam kerja yang dilakukan untuk menurunkan risiko akibat kesilapan manusia.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MPB yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
b) Memastikan pegawai dan kakitangan MPB serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MPB;

c) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPB secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;
d) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan MPB sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MPB; dan
e) 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 Seksyen Pengurusan Sumber Manusia.

Tindakan : PSM, TMK dan Semua

040103 Tamat Perkhidmatan atau Pertukaran Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a) Memastikan semua aset ICT dikembalikan kepada MPB mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
b) Membatalkan, menggantung atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MPB atau terma perkhidmatan.

Tindakan : PTA & TMK

BIDANG 05 - KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

Objektif :

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

050101 Keselamatan Kawasan Fizikal

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

Perkara-perkara yang perlu dipatuhi bergantung kepada hasil penilaian risiko termasuk yang berikut :

a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset;
b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
c) Memasang alat penggera atau kamera;
d) Menghadkan jalan keluar masuk;
e) Mengadakan kaunter kawalan;
f) Mewujudkan perkhidmatan kawalan keselamatan;
g) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
h) Menyediakan garis panduan untuk kakitangan yang bekerja di kawasan terhad; dan
i) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.

Tindakan : PTA, CIO dan ICTSO

050102 Kawalan Masuk Fizikal

Kawalan Masuk Fizikal perlu dikenal pasti dan dilaksanakan ke atas kawasan yang menempatkan infrastruktur rangkaian dan komunikasi, fasiliti pemprosesan atau tempat penyimpanan maklumat terperingkat.

Keselamatan fizikal termasuk keselamatan perimeter seperti pembinaan dinding, pagar kawalan dan menghadkan jalan keluar masuk ke kawasan berkenaan.

Akses ke kawasan pejabat dan kawasan larangan perlu dikawal bagi memastikan hanya kakitangan atau pihak yang diberi tanggungjawab sahaja dibenarkan masuk.

Tindakan : PTA dan Semua

050103 Kawasan Larangan ICT

Kawasan larangan ditakrifkan sebagai kawasan dimana terdapat aset ICT kritikal yang boleh menjejaskan operasi dan keselamatan maklumat secara keseluruhan jika tidak dikawal.

Kawasan larangan ICT di MPB ialah Bilik Server. Akses kepada kawasan larangan hendaklah dikawal dan kebenaran hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan 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 dipantau sepanjang masa sehingga tugas di kawasan berkenaan selesai.

Tindakan : TMK, PTA dan Semua

050104 Perlindungan Kawasan ICT Dari Ancaman Luar Dan Bencana Alam

Kawalan dan perlindungan keselamatan ke atas kawasan ICT perlu mengambilkira ancaman dari perbuatan manusia ataupun kebakaran.

Tindakan : TMK, PTA dan Semua

050105 Kawalan Kawasan Penghantaran Barangan dan *Loading Area*

Kawasan penghantaran barangan dan *loading area* hendaklah dikawal dan perlu dipisahkan dari akses terus ke kawasan larangan.

Tindakan : PTA dan Semua

0502 Keselamatan Aset ICT

Objektif:

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

050201 Peralatan dan Perkakasan ICT

Semua aset ICT perlu dijaga dan dikawal dengan baik supaya ianya boleh digunakan sepanjang masa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Pengguna hendaklah menyemak dan memastikan semua aset ICT di bawah kawalannya berfungsi dengan sempurna;
b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;
c) Pengguna dilarang sama sekali menambah, menuntut atau mengganti sebarang pekakasan ICT yang telah ditetapkan;
d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir ICT;
e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;
f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini disamping melakukan imbasan ke atas media storan yang digunakan;
g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;
h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;
i) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan.
j) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin atau mempunyai pengudaraan (*air ventilation)* yang sesuai;
k) Peralatan ICT yang hendak dibawa keluar dari premis MPB perlulah mendapat kelulusan oleh pegawai yang diberikan kuasa dan direkodkan bagi tujuan pemantauan;

l) Peralatan ICT yang hilang hendaklah dilaporkan kepada Pegawai Aset dengan segera;
m) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;
n) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal (dalam pejabat/bahagian yang sama) ia ditempatkan tanpa kebenaran Ketua Bahagian/Ketua Pejabat Cawangan/Ketua Unit;
o) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir ICT untuk dibaik pulih;
p) Sebarang pelekat selain tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;
q) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;
r) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir ICT;
s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;
t) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF” apabila meninggalkan pejabat;
u) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan
v) Memastikan suis ditutup bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

Tindakan : Semua

050202 Media Storan Digital

Media storan digital merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cekera padat, pita magnetik, optical disk, flash disk, CDROM, thumb drive dan media storan lain.

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

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;
c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;
e) Perkakasan backup hendaklah diletakkan di tempat yang terkawal;
f) Mengadakan salinan atau penduaan (backup) bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; dan
g) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat.

Tindakan : Semua

050203 Media Tandatangan Digital

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;
b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan
c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan selanjutnya.

Tindakan : Semua

050204 Media Perisian dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MPB;
b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran CIO;
c) Lesen perisian daripada CD-rom, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan
d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

Tindakan : Semua

050205 Utiliti Sokongan

Semua utiliti sokongan perlu berada dalam keadaan terbaik dan mencukupi bagi menyokong sistem beroperasi. Utiliti sokongan ini termasuk bekalan elektrik, air, penghawa dingin, generator, alat komunikasi dan lain-lain.

Tindakan : Semua

050206 Penyelenggaraan Perkakasan

Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti adalah terkawal. Perkara-perkara yang perlu dipatuhi termasuk yang tersenarai di bawah:

a) Semua perkakasan perlu diselenggara mengikut spesifikasi yang telah ditetapkan oleh pengeluar;
b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;
c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;
d) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan
e) Semua penyelenggaraan mestilah mendapat kebenaran daripada pegawai yang diberikan tanggungjawab menjaganya.

Tindakan : Semua

050207 Aset ICT di Luar Premis

Aset ICT seperti storan penyimpanan maklumat, komputer peribadi, *computer tablet*, telefon mudah alih, *smart card*, dokumen atau lain-lain perkakasan yang dibawa keluar premis MPB perlu dilindungi dari risiko keselamatan seperti kecurian, kerosakan dan lain-lain.

Antara perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Aset yang hendak dibawa keluar dari premis perlu mendapat kebenaran;
b) Pegawai adalah bertanggungjawab sepenuhnya ke atas aset yang dibawa keluar;
c) Aset perlu dilindungi dan dikawal sepanjang masa;
d) Maklumat pada aset hendaklah sentiasa dilindungi oleh katakunci ; dan
e) Penyimpanan atau penempatan aset mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

Tindakan : Semua

050208 Pelupusan dan Guna Semula Perkakasan

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

Aset ICT yang akan dilupuskan atau diguna semula, terutama yang mengandungi maklumat terperingkat atau perisian yang dilesenkan, perlu diuruskan dengan teratur dan selamat mengikut prosedur pelupusan semasa atau guna semula peralatan yang telah ditetapkan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPB.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Semua kandungan perkakasan khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan atau diguna semula;
b) Pelupusan Aset ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa kecuali Pejabat Wilayah Sabah dan Pejabat Wilayah Semenanjung Malaysia;
c) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan;

d) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;
e) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;
f) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
g) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
h) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori; dan
i) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk, motherboard* dan sebagainya;
ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian MPB;
iii. Memindah keluar dari MPB mana-mana peralatan ICT yang hendak dilupuskan;
iv. Melupuskan sendiri peralatan ICT; dan
v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti thumb drive atau external hard disk sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

Tindakan : TMK dan Semua

0503 Keselamatan Persekitaran

Objektif:

Melindungi aset ICT MPB dari sebarang bentuk ancaman persekitaran yang disebabkan oleh kebakaran, kesilapan, kecuaian 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 Ketua Bahagian Pengurusan Sumber Manusia dan Pentadbiran Am.

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

i. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran;
ii. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
iii. Bahan mudah terbakar hendaklah disimpan di luar kawasan bersesuaian dan berjauhan dari aset ICT;
iv. Semua cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; dan
v. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya satu (1) kali setahun. Aktiviti dan keputusan ujian ini pelu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.

Tindakan : PTA dan Semua

050302 Bekalan Kuasa

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

(a) Semua peralatan ICT kritikal hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;
(b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan/atau penjana (*generator)* hendaklah digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan ; dan
(c) Semua peralatan sokongan bekalan kuasa di Bilik Server hendaklah diperiksa dan diuji secara berjadual.

Tindakan : TMK

050303 Kabel

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

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

a) Menggunakan kabel yang mengikuti spesifikasi yang telah ditetapkan;
b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan; dan
d) Semua kabel perlu dilabelkan dengan jelas pada network port socket outlet (*face plate*).

Tindakan : TMK

050304 Prosedur Kecemasan Kebakaran

Prosedur kecemasan persekitaran seperti kebakaran yang melibatkan persekitaran kawasan ICT terjejas hendaklah di kaji dari masa ke masa.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan semasa MPB; dan
b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Ketua Seksyen Pentadbiran Am atau *Floor Warden*, Pasukan Tindakan Kecemasan MPB.

Tindakan : PTA

0504 Keselamatan Dokumen

Objektif:

Melindungi maklumat MPB dari sebarang bentuk ancaman persekitaran yang disebabkan oleh kebakaran, kesilapan atau kecuaian.

050401 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;
b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;
c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut Prosedur Arahan Keselamatan;
d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa sepertimana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan
e) Menggunakan enkripsi (*encryption)* ke atas dokumen pembayaran perbankan yang dihantar secara elektronik.

Tindakan : Semua

BIDANG 06 – PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur Operasi dan Tanggungjawab

Objektif:

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

060101 Pengendalian Prosedur Operasi ICT

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal;
b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan
c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan, diberikan nombor versi pindaan dan diluluskan oleh Pengurus ICT.

Tindakan : Semua

060102 Kawalan Perubahan

Perubahan yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah dikemukakan oleh pemilik sistem atau pentadbir rangkaian dan komunikasi dan mendapat kebenaran daripada pegawai yang diberi kuasa; dan

Sebarang perubahan komponen sistem ICT hendaklah mematuhi keperluan yang ditetapkan.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

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

b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

Tindakan : Semua

060103 Pengasingan Tugas dan Tanggungjawab

Tugas dan tanggungjawab setiap pegawai perlu ditetapkan dan jelas bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan
c) Perkakasan yang digunakan bagi membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production.*

Tindakan : Pengurus ICT/ ICTSO

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif:

Memastikan penyampaian perkhidmatan pihak ketiga mematuhi tahap keselamatan yang ditetapkan selaras dengan perjanjian perkhidmatan.

060201 Perkhidmatan

Pihak ketiga perlu mematuhi terma dan syarat-syarat berkaitan kawalan keselamatan yang telah ditetapkan dalam perjanjian.

Perkara-perkara yang mesti dipatuhi adalah seperti berikut :

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

Tindakan : Pengurus ICT dan Semua

060202 Pemantauan Perkhidmatan Pihak Ketiga

Perkhidmatan, laporan dan rekod pihak ketiga perlu dipantau dan disemak.

Tindakan : Pengurus ICT

0603 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

060301 Pengurusan Kapasiti

Pengurusan kapasiti perlu dilaksanakan sebelum sistem dibangun dan dilaksanakan dengan mengambilkira keperluan selama 3 tahun.

Tindakan : Pentadbir ICT

060302 Perancangan Kapasiti

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang.

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

060303 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

Sijil penerimaan sistem hanya akan dikeluarkan setelah segala ujian penerimaan yang ditetapkan berjaya dilaksanakan sepenuhnya.

Tindakan : Pentadbir ICT

0604 Kawalan Terhadap Perisian Berbahaya

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

060401 Perlindungan Dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Instrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;
b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa;
c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;
d) Mengemaskini anti virus dengan *pattern* antivirus yang terkini;
e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
g) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

Tindakan : Semua

060402 Kawalan terhadap kod berbahaya (*Malicious Code)*

Perisian atau sistem yang digunakan mesti bebas daripada kod berbahaya (*malicious code)*

Tindakan : Pentadbir ICT

060403 Kawalan terhadap *Mobile Code*

Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

Tindakan : Pentadbir ICT

0605 Housekeeping (Back Up)

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 mengikut prosedur yang telah ditetapkan.

Perkara-perkara yang perlu dicontohi adalah seperti berikut:

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

Tindakan : Pengurus ICT dan Semua Pentadbir ICT

0606 Pengurusan Keselamatan Rangkaian

Objektif:

Memastikan maklumat dan infrastruktur rangkaian dilindungi.

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 yang berikut:

a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan ;
b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;
c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
d) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian;
e) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MPB;
f) Semua peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai antivirus yang sah;
g) Capaian kepada rangkaian perlu dilaksanakan mengikut kategori yang telah ditetapkan iaitu Intranet, Internet dan DMZ;
h) Peralatan persendirian adalah dilarang untuk capaian kepada rangkaian Intranet MPB;
i) Pihak ketiga adalah tidak dibenarkan untuk mencapai rangkaian Intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran pemilik sistem; dan

Tindakan : Pengurus ICT, ICTSO dan Pentadbir Rangkaian

0607 Pengendalian Media

Objektif:

Melindungi media mudah alih dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan perkhidmatan.

060701 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu dan perlu mematuhi prosedur yang ditetapkan.

Tindakan : Semua

060702 Prosedur Pengendalian Dan Pelupusan Media

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

a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat ;
b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;
c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;
d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;
e) Menyimpan semua media di tempat yang selamat; dan
f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.

Tindakan : Semua

060703 Keselamatan Sistem Dokumentasi

Sistem dokumentasi perlu disimpan dengan selamat dan dilindungi daripada capaian yang tidak dibenarkan.

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

a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;
b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan
c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.

Tindakan : Semua

0608 Pengurusan Pertukaran Maklumat

Objektif:

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

060801 Pertukaran Maklumat

Pertukaran maklumat mesti mendapat kelulusan dari pihak pengurusan.

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 MPB dengan agensi luar;
c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MPB; dan
d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.

Tindakan : Semua

060802 Pengurusan Mel Elektronik (E-mel)

Penggunaan e-mel hendaklah mematuhi etika dan peraturan yang ditetapkan oleh MPB.

Pengguna e-mel perlu mematuhi perkara berikut:

a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukan oleh MPB sahaja boleh digunakan semasa membuat urusan rasmi;
b) Penggunaan akaun milik orang lain adalah dilarang;
c) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; dan
d) Pengguna perlu memastikan semua e-mail dibaca dan diambil tindakan segera.

Tindakan : Semua

060803 Business Information System

Maklumat yang terlibat dalam perkongsian data di antara sistem aplikasi perlu dilindungi.

Tindakan : Semua

060804 Kawalan Media Sosial

Semua akaun media sosial berkaitan aktiviti bahagian/unit MPB hendaklah mendapat kelulusan Jawatankuasa Pemandu ICT (JPICT) dan ditadbir oleh Bahagian/Unit tersebut.

Tindakan : Semua

0609 Perkhidmatan Transaksi Atas Talian

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 Transaksi Atas Talian

Maklumat yang terlibat dalam transaksi atas talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian dan pendedahan yang tidak dibenarkan. Penggunaan EFT (Electronic Fund Transfer) hendaklah mengikut amalan terbaik keselamatan transaksi atas talian seperti di dalam dokumen ini.

Tindakan : Pemilik Sistem dan Pentadbir Sistem

060902 Maklumat Capaian Umum

Maklumat yang dipaparkan perlu mempunyai tahap integriti yang tinggi dan dilindungi dari pindaan yang tidak dibenarkan.

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

a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;
b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan
c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.

Tindakan : Pentadbir Laman Web dan Semua

0610 Pemantauan

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

061001 Pengauditan dan Forensik ICT

Pentadbir ICT mestilah bertanggungjawab mengesan, merekod dan menganalisis perkara-perkara berikut :

a) Sebarang percubaan pencerobohan kepada sistem ICT MPB;
b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery phising*), pencerobohan (*instrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);
c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;
d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;
e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;
f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar *(bandwitdth*) rangkaian;
g) Aktiviti penyalahgunaan akaun e-mel; dan
h) Aktiviti penukaran alamat IP (IP address) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir ICT.

Tindakan : ICTSO dan Pentadbir ICT

061002 Jejak Audit

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

Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

a) Rekod setiap aktiviti transaksi;

b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;
c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Jejak audit hendaklah disimpan untuk tempoh masa yang ditetapkan pihak pengurusan atau peraturan semasa.

Pentadbir 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.

Tindakan : Pentadbir ICT

061003 Sistem Log

Bagi memastikan aktiviti sistem kritikal dipantau, Pentadbir ICT perlu melaksanakan perkara-perkara berikut:

a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan
c) Sekiranya wujud aktiviti-aktiviti yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan kepada Ketua Bahagian ICT dan CIO.

Tindakan : Pentadbir ICT

061004 Pemantauan Log

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;
c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;
d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;
e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan
f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MPB atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

Tindakan : Pentadbir ICT

061005 Perlindungan Log

Maklumat dan fasiliti log perlu dilindungi daripada capaian yang tidak dibenarkan.

Tindakan : Pentadbir ICT

061006 Log untuk Pentadbir Sistem

Segala aktiviti pentadbir dan operator sistem perlu direkod.

Tindakan : Pentadbir ICT

061007 Log Kerosakan

Segala kerosakan perlu direkod, dianalisa dan diambil tindakan.

Tindakan : Pentadbir ICT

061008 Penyeragaman Waktu

Semua sistem ICT MPB perlu mempunyai waktu yang seragam dengan *Network Time Protokol* (NTP) atau waktu yang dinyatakan oleh SIRIM.

Tindakan : Pentadbir ICT

BIDANG 07 - KAWALAN CAPAIAN

0701 Kawalan Capaian

Objektif:

Memastikan capaian kepada maklumat adalah berdasarkan kepada keperluan organisasi dan keselamatan maklumat.

070101 Keperluan Kawalan Capaian

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;
b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan
d) Kawalan ke atas kemudahan pemprosesan maklumat

Tindakan : Pentadbir ICT

0702 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT MPB

070201 Pendaftaran Akaun Pengguna

Pendaftaran, pengemaskinian dan penamatan akaun penguna mestilah dilaksanakan mengikut prosedur yang ditetapkan. Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:

a) Akaun pengguna hanya diwujudkan setelah mendapat pengesahan Seksyen Pengurusan Sumber Manusia dan pengguna telah mengesahkan memahami Dasar Keselamatan ICT;
b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;
c) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem terlebih dahulu;
d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MPB. Akaun boleh ditarik balik jika penggunaanya melanggar peraturan;
e) Penggunaan akaun milik orang lain adalah dilarang;
f) Penggunaan akaun tidak boleh dikongsi; dan
g) Akaun pengguna boleh dibeku atau ditamatkan apabila menerima arahan daripada Seksyen Pengurusan Sumber Manusia atas sebab-sebab berikut:
    i. Bersara;
    ii. Bertukar secara tetap ke agensi lain;
    iii. Bagi menjalankan siasatan; atau
    iv. Ditamatkan perkhidmatan

Tindakan : Semua

070202 Hak Capaian *(Privilege)*

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

Tindakan : Pemilik Sistem dan Pentadbir ICT

070203 Semakan Hak Capaian Pengguna

Pemilik sistem perlu menyemak semula hak capaian pengguna dari semasa ke semasa.

Tindakan : Pentadbir ICT

070204 Pengurusan Kata Laluan Pengguna

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta garispanduan yang ditetapkan oleh MPB.

Tindakan : Semua

0703 Tanggungjawab Pengguna

Objektif:

Menghalang capaian yang tidak dibenarkan terhadap maklumat dan fasiliti pemprosesan.

070301 Penggunaan Akaun dan Kata Laluan

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

b. Pengguna hendaklah menukar kata laluan sekurang-kurangnya sekali dalam tempoh setahun atau apabila disyaki berlakunya kebocoran kata laluan atau dikompromi.

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

d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun.

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

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

g. Tentukan had masa pengesahan selama lima (5) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan, dan

h. Mengelakkan penggunaan semula kata laluan yang lama digunakan.

Tindakan : Semua

070302 Unattended User Equipment

a) Komputer yang *idle* dalam tempoh 5 minit perlu di *lock screen*;
b) Semua peralatan komputer perlu di *log off* setelah tugasan selesai; dan
c) Kawalan yang bersesuaian perlu dilaksanakan bagi peralatan tanpa pengawasan.

Tindakan : Semua

070303 Clear Desk dan Clear Screen

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

a) Pengguna perlu *lock screen* apabila meninggalkan komputer pada bila-bila masa;
b) Semua fail atau dokumen terperingkat perlu disimpan di tempat yang berkunci apabila meninggalkan meja kerja;
c) Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.; dan
d) Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

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

Tindakan : Semua

070304 Penggunaan Komputer/Notebook

Penggunaan aset komputer MPB termasuk desktop *dan notebook* perlu dikawal supaya tiada pencerobohan, penyalahgunaan, kecurian, kehilangan dan pengubahsuaian kepada maklumat.

Semua pengguna komputer MPB perlu mematuhi perkara berikut:

a) Semua komputer MPB hendaklah digunakan untuk tugas rasmi sahaja;
b) Pengguna bertanggungjawab memastikan bahawa komputer perlu sentiasa mempunyai *antivirus* yang aktif dan terkini;
c) Semua komputer perlu didaftar pemiliknya dan pemilik berkenaan adalah bertanggungjawab menjaga keselamatan komputer tersebut;
d) Ketua Bahagian/Pengarah Wilayah/Ketua Pejabat Cawangan/Unit adalah bertanggungjawab terhadap notebook gunasama, dan setiap pergerakan notebook tersebut perlu direkodkan;
e) Komputer (notebook) yang dibekalkan kepada pegawai yang layak, dibenarkan untuk dibawa pulang atau dibawa ke mana-mana dan pegawai adalah bertanggungjawab menjaga keselamatan aset berkenaan sepanjang masa;
f) Pentadbir ICT berhak untuk menyiasat kandungan komputer apabila menerima arahan daripada CIO;
g) Komputer milik MPB saja yang dibenarkan untuk mencapai maklumat-maklumat yang terdapat di dalam Intranet;
h) Komputer milik MPB adalah dilarang digunakan oleh pihak ketiga tanpa kawalan dan pengawasan pegawai MPB; dan
i) Pegawai Aset perlu melaporkan dengan segera sekiranya berlaku kehilangan komputer atau notebook kepada CIO dengan menyertakan salinan laporan polis.

Tindakan : Semua

0704 Kawalan Capaian Rangkaian

Objektif:

Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas perkhidmatan Rangkaian (wayar dan tanpa wayar) MPB.

070401 Capaian Rangkaian

Penggunaan perkhidmatan rangkaian diberikan kepada pengguna berasaskan kepada tugas dan skop kerja. Semua sistem/aplikasi atau pengguna perlu mematuhi kawalan capaian perkhidmatan rangkaian yang ditetapkan seperti berikut;

a) Semua capaian akan berasaskan kepada 3 zone rangkaian iaitu Intranet, *Demilitarized Zone* (DMZ) dan Internet ;
b) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MPB, rangkaian agensi lain dan rangkaian awam;
c) Menghalang mana-mana pengguna awam memasuki ke rangkaian intranet tanpa pengawasan;
d) Kontraktor atau pihak ketiga adalah dilarang membawa keluar peralatan yang digunakan untuk mencapai rangkaian intranet kecuali telah mendapat pengesahan pemilik sistem; dan
e) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

Tindakan : Pentadbir Rangkaian, Pengurus ICT dan Semua

070402 Capaian Internet

Capaian melalui Internet (Rangkaian Awam) kepada rangkaian dan maklumat MPB hendaklah dikawal bagi memastikan tiada berlaku kecurian, pencerobohan, kerosakan dan pengubahsuaian.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Capaian ke Intranet MPB menggunakan Internet atau rangkaian awam adalah tidak dibenarkan;
b) Penggunaan Internet di MPB hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja seperti yang terdapat di dalam tatacara penggunaan Internet;
c) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. ICTSO berhak menentukan penggunaan yang dibenarkan atau sebaliknya;
d) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh ICTSO atau CIO ;
e) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian sebelum dimuat naik ke Internet;
f) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;
g) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MPB;
h) Penggunaan modem/broadband pada mana-mana peralatan atau aset yang berada atau bersambung dengan rangkaian MPB adalah tidak dibenarkan sama sekali; dan
i) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut;

    i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video dan 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.

Tindakan : Pentadbir Rangkaian, Pengurus ICT, Semua

070403 Peralatan Dalam Rangkaian

Bagi memastikan bahawa peralatan yang disambungkan kepada Rangkaian MPB tidak menjejaskan keselamatan maklumat dan capaian, maka perkara-perkara berikut hendaklah dipatuhi:

a) Semua peralatan perlu disahkan bebas daripada virus dan perisian antivirus hendaklah dipasang dan masih aktif sepanjang masa; dan
b) Setiap peralatan yang hendak disambung ke rangkaian perlu menggunakan protocol TCP/IP dan akan menggunakan *IP address* atau *domain name* yang ditetapkan oleh Pentadbir Rangkaian.

Tindakan : Pentadbir Rangkaian

070404 Capaian ke atas Port Untuk Tujuan Diagnostik

Bagi memastikan bahawa port rangkaian tidak dicapai tanpa pengawasan, perkara berikut perlu dipatuhi oleh semua pengguna;

a) Semua port yang tidak digunakan perlu di *disable*;
b) Capaian fizikal dan logikal ke atas port untuk tujuan diagnostik perlu mendapat kebenaran pegawai yang diberikan kuasa;
c) Capaian oleh pegawai MPB hanya dibenarkan berasaskan kepada tugas dan skop kerja; dan
d) Capaian oleh pihak ketiga perlu mendapat kelulusan dari pegawai yang diberikan kuasa.

Tindakan : Pentadbir Rangkaian

070405 Pengasingan Dalam Rangkaian

Rangkaian MPB perlu dibuat pengasingan menggunakan VLAN, Zon (Intranet, DMZ, Internet) dan VPN mengikut jenis perkhidmatan, pengguna, sensitiviti maklumat dan sistem.

Tindakan : Pentadbir Rangkaian

070406 Kawalan Penghalaan *(Routing)* Rangkaian

Penghalaan perlu dikawal supaya ianya tidak disalah guna dengan memastikan perkara berikut:

a) Konfigurasi routing perlu disemak dan disahkan sebelum dilaksanakan;
b) Semakan *routing table* perlu dibuat dari semasa ke semasa; dan
c) Penghalaan (Routing) di dalam sistem rangkaian perlu dilaksanakan dengan betul dan terkawal.

Tindakan : Pentadbir Rangkaian

0705 Kawalan Capaian Sistem Pengoperasian

Objektif:

Menghalang capaian yang tidak sah dan tanpa dibenarkan ke atas sistem pengoperasian.

070501 Capaian Sistem Pengoperasian

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

a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan
b) Merekodkan capaian yang berjaya dan gagal.

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

a) Mengesahkan pengguna yang dibenarkan;
b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin;
ii. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;
iii. Menghadkan dan mengawal penggunaan program; dan
iv. Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

Tindakan : Pentadbir ICT

070502 Secure Log-on

Log-on ke atas sistem pengoperasian perlu melalui satu kaedah yang selamat bagi mengurangkan akses yang tidak dibenarkan.

Tindakan : Pentadbir ICT

070503 Pengenalan dan Pengesahan Pengguna

Capaian masuk sistem perlu mempunyai kaedah bagi mengenal dan mengesahkan pengguna adalah sah.

Tindakan : Pentadbir ICT

070504 Penggunaan Sistem Utiliti

Penggunaan sistem utiliti perlulah dikawal dan dihad kepada pegawai yang dibenarkan saja.

Tindakan : Pentadbir ICT

070505 Session Time-Out

Sesi yang tidak aktif perlu ditamatkan mengikut tempoh masa yang ditetapkan.

Tindakan : Pentadbir Sistem Aplikasi dan Pentadbir Rangkaian

070506 Had Masa Capaian

a) Had masa capaian kepada maklumat dan sistem aplikasi hendaklah berasaskan kepada keperluan dan fungsi pengguna;
b) Masa capaian bagi aplikasi berisiko tinggi perlu dihadkan semasa waktu pejabat sahaja

Tindakan : Pentadbir Sistem Aplikasi

0706 Kawalan Capaian Aplikasi dan Maklumat

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

070601 Capaian Aplikasi dan Maklumat

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

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

a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang diberikan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;
b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);
c) Menghadkan capaian sistem dan aplikasi kepada lima (5) kali percubaan.;
d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan
e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja dan di dalam zon yang ditetapkan.

Tindakan : Semua

070602 Larangan Capaian Maklumat

a) Capaian kepada maklumat dan sistem aplikasi hendaklah berasaskan kepada keperluan dan fungsi pengguna;
b) Capaian kepada maklumat yang tidak rasmi , berunsur lucah, iklan dan yang menjejaskan prestasi kerja; dan
c) Capaian kepada maklumat dan sistem aplikasi perlu dinyatakan dengan jelas kepada pengguna.

Tindakan : Semua

070603 Pengasingan Sistem Kritikal

Pengasingan sistem kritikal perlu dilaksana dengan menggunakan VLAN/ VPN dan zon rangkaian (Intranet, DMZ, Internet)

Tindakan : Pentadbir Rangkaian

0707 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif:

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

070701 Peralatan Mudah Alih

Perkara yang perlu dipatuhi adalah seperti berikut :

a) Peralatan mudah alih yang dikhaskan untuk pegawai yang berkelayakan dibenarkan dibawa keluar bagi melaksanakan tugas-tugas rasmi;
b) Peralatan mudah alih gunasama perlu direkod dan mendapat kelulusan pegawai yang bertanggungjawab apabila hendak dibawa keluar dari pejabat;
c) Semua peralatan mudah alih hendaklah dilindungi dan dikawal dengan selamat; dan
d) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

Tindakan : Semua

070702 Kemudahan Kerja Jarak Jauh

Kerja Jarak Jauh hanya boleh dilaksanakan setelah mendapat kelulusan pegawai yang diberi kuasa dan pemilik sistem yang berkaitan.

Perkara yang perlu dipatuhi adalah seperti berikut :

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

Tindakan : Semua

BIDANG 08 - PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif :

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

080101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh menggangu pemprosesan dan ketetapan maklumat;
b) Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem *output* untuk memastikan data yang telah diproses adalah tepat;
c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan
d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.

Tindakan : Pentadbir Sistem Aplikasi, Pemilik Sistem dan ICTSO

080102 Analisa Dan Spesifikasi Keperluan Keselamatan

Spesifikasi reka bentuk perlu memasukkan keperluan keselamatan sistem maklumat. Sekiranya sesuatu *off-the-shelf* produk diperolehi, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.

Tindakan : Pentadbir Sistem Aplikasi

0802 Kebolehpercayaan Pemprosesan Dalam Aplikasi

Objektif:
Untuk mengelak kesalahan, kecacatan, kerugian, pengubahsuaian yang tidak dibenarkan, penyalahgunaan maklumat dalam aplikasi atau kehilangan kepercayaan terhadap sistem.

080201 Pengesahan Data *Input*

Data yang dimasukkan ke dalam aplikasi perlu disahkan untuk memastikan data adalah tepat dan betul.

Tindakan : Pemilik Sistem

080202 Kawalan Bagi Pemprosesan Dalaman

Satu prosedur semakan perlu diadakan di dalam aplikasi bagi mengesan sebarang kerosakan maklumat yang terhasil dari kesilapan dan kecacatan pemprosesan ataupun kesalahan yang disengajakan. Senarai semak yang bersesuaian perlu disediakan, aktiviti-aktiviti didokumenkan dan hasil keputusan perlu disimpan dengan selamat.

Tindakan : Pentadbir Sistem Aplikasi

080203 Integriti Maklumat

Satu penilaian terhadap risiko keselamatan perlu dijalankan untuk menentukan keperluan integriti maklumat dan bagi mengenal pasti kaedah yang paling bersesuaian untuk dilaksanakan.

Tindakan : Pemilik Sistem dan Pentadbir Sistem Aplikasi

080204 Pengesahan Data *Output*

Data yang dikeluarkan daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

Tindakan : Pemilik Sistem

0803 Kawalan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi mengikut keperluan.

080301 Enkripsi

Proses enkripsi (*encryption*) perlu dilaksanakan bagi melindungi kerahsiaan maklumat kritikal atau sensitif berdasarkan keperluan, penilaian risiko dan selaras dengan Akta-akta MPB.

Tindakan : Semua

080302 Tandatangan Digital

Penggunaan tandatangan digital (sekiranya berkaitan) adalah dimestikan kepada semua pengguna khususnya yang berurusan dengan transaksi maklumat kritikal atau sensitif atau maklumat rahsia rasmi secara elektronik.

Tindakan : Semua

080303 Pengurusan Kunci Kriptografi

Pengurusan ke atas kunci kriptografi yang dilaksanakan ke atas maklumat kritikal atau sensitif hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

Tindakan : Semua

0804 Keselamatan Fail Sistem

Objektif:

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

080401 Kawalan Perisian (*Operational Software*)

Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Proses pengemaskinian perisian hanya boleh dilakukan oleh Pentadbir ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan;
b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan untuk digunakan;
c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan;
d) Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan
e) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal.

Semua sistem konfigurasi perlu didokumenkan/daftarkan.

Tindakan : Pentadbir ICT

080402 Kawalan Data Pengujian Sistem

Data pengujian sistem perlu dipilih dengan teliti, dilindungi dan terkawal. Penggunaan data sebenar (*operational data*) yang melibatkan data personel atau data sensitif pada persekitaran pengujian perlu dielakkan. Jika data personel atau data sensitif digunakan untuk tujuan pengujian, kandungan sensitif perlu ditapis atau diubahsuai sebelum digunakan.

Tindakan : Pemilik Sistem

080403 Kawalan Capaian kepada Kod Sumber (*Source Code*)

Kawalan capaian kepada kod atau atur cara program perlu dilaksanakan bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian.

Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik MPB.

Tindakan : Pentadbir Sistem Aplikasi

0805 Keselamatan Dalam Proses Pembangunan dan Prosesan Sokongan

Objektif:

Menjaga dan menjamin keselamatan sistem perisian aplikasi dan maklumat.

080501 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dikawal, diuji, direkodkan dan disahkan melalui prosedur yang ditetapkan sebelum diguna pakai;
b) Pengujian terhadap perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dilaksanakan dalam persekitaran yang berasingan samada daripada produksi atau pembangunan;
c) 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;
d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;
e) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan
f) Menghalang sebarang peluang untuk membocorkan maklumat.

Tindakan : Pentadbir Sistem Aplikasi dan Pemilik Sistem

080502 Keperluan Kajian Teknikal Terhadap Aplikasi Selepas Perubahan Sistem Pengoperasian

Semua aplikasi perlu dikaji dan diuji apabila berlaku perubahan sistem pengoperasian bagi memastikan tiada sebarang kesan buruk yang merugikan kepada operasi dan keselamatan organisasi.

Tindakan : Pentadbir Sistem Aplikasi

080503 Pembangunan Perisian Secara *Outsource*

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

Tindakan: Pemilik Sistem dan Pentadbir Sistem

0806 Pengurusan Kelemahan Teknikal

Objektif:

Mengurangkan Risiko Akibat Dari Eksploitasi Kelemahan Teknikal.

080601 Kawalan Kelemahan Teknikal

Kelemahan teknikal terhadap sistem maklumat perlu dilapor dan dibuat penilaian dengan segera untuk tindakan pembetulan.

Tindakan : Pemilik Sistem dan Pentadbir Sistem Aplikasi

0807 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Objektif:

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

080701 Kawalan dari Ancaman Teknikal

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

Perkara yang perlu dipatuhi adalah seperti berikut :

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

Tindakan : Pentadbir Sistem

BIDANG 09 - PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

Memastikan insiden keselamatan ICT dan kelemahan dilapor dan disalur dengan cepat dan berkesan bagi meminimumkan proses pembaikan dan mengurangkan 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 CERT MPB dengan kadar segera:

a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.

Prosedur pelaporan insiden keselamatan ICT berdasarkan:

(a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi.

(b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

Tindakan : Semua

090102 Pelaporan Kelemahan Keselamatan

Pengguna sistem dikehendaki melaporkan sebarang kelemahan sistem dengan segera bagi mengelak insiden keselamatan ICT.

Tindakan : Semua

0902 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

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

090201 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 MPB.

Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan.

Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut :

a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;
b) Menyalin bahan bukti dan merekodkan semua maklumat dan aktiviti penyalinan;
c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;
d) Menyediakan tindakan pemulihan segera; dan
e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

Tindakan : CIO dan Pengurus ICT

090202 Pembelajaran Dari Insiden Kelemahan Maklumat

Mewujudkan mekanisma bagi menentukan semua insiden keselamatan maklumat direkod untuk dianalisa dan dipantau.

Tindakan : ICTSO dan Pentadbir Sistem Aplikasi

090203 Pengumpulan Bukti

Bukti-bukti insiden keselamatan maklumat perlu dikumpul dan dikekalkan untuk tindakan perundangan.

Tindakan : ICTSO dan Pentadbir Sistem Aplikasi

BIDANG 10 - PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

Objektif:

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

100101 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan/ BCP*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan.

Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh pihak pengurusan MPB atau mana-mana jawatankuasa yang ditubuhkan. Perkara-perkara berikut perlu diberi perhatian:

a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;
c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
d) Mendokumentasikan proses dan prosedur yang telah dipersetujui;
e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
f) Membuat *backup*; dan
g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

BCP mempunyai empat komponen utama iaitu:-

a) Pelan Pemulihan Bencana;
b) Pelan Tindakbalas Kecemasan;
c) Pelan Tindakbalas Insiden; dan
d) Pelan Komunikasi.

DAN hendaklah mengandungi perkara-perkara berikut:

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

Salinan BCP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP 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 BCP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. MPB hendaklah memastikan salinan BCP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

Tindakan : TMK/PTA/KEW

BIDANG 11 – PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif:

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

110101 Pematuhan Dasar

Setiap pengguna di MPB hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MPB dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.

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

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

Tindakan : Semua

110102 Pematuhan dengan Dasar dan Keperluan Teknikal

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

Tindakan : ICTSO

110103 Pematuhan Keperluan Audit

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

Tindakan : Semua

110104 Keperluan Perundangan

Semua pengguna aset ICT MPB perlu mematuhi segala keperluan perundangan, akta atau peraturan-peraturan lain yang berkaitan yang terpakai oleh MPB.

Senarai Perundangan dan Peraturan adalah seperti berikut:

1. Dasar Keselamatan ICT MPB (DKICT)
2. Pekeliling Am Bil.4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam
3. Surat Pekeliling Am Bil.4 Tahun 2022 – Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam
4. Surat Pekeliling Am Bil.3 Tahun 2022 – Garis Panduan Pengurusan Keselamatan Penggunaan Persidangan Video (Video Conferencing) Dalam Perkhidmatan Awam
5. Surat Pekeliling Am Bil.2 Tahun 2021 – Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam
6. Surat Pekeliling Am Bil.1 Tahun 2020 – Pemakluman Pemakaian dan Penguatkuasaan Arahan Keselamatan (Semakan dan Pindaan 2017)
7. Pekeliling Am Bil.1/2015 – Pelaksanaan Data Terbuka Sektor Awam
8. Surat Pekeliling Am Bil. 3 Tahun 2015 – Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam
9. Pekeliling Kemajuan Pentadbiran Awam Bil.2 Tahun 2015 – Pengurusan Laman Web Agensi Sektor Awam
10. Surat Pekeliling Am Bil.3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam
11. Arahan Teknologi Maklumat (Dis 2007)
12. Surat Pekeliling Am Bil.4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
13. Pekeliling Am Bil.3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
14. Akta Tandatangan Digital 1997 (Akta 562)
15. Akta Jenayah Komputer (Akta 563)
16. Akta Hak Cipta 1987 (Akta 332)
17. Akta Rahsia Rasmi 1972 (Akta 88)

Tindakan : Semua

110105 Pelanggaran Dasar

Pelanggaran Dasar Keselamatan ICT MPB boleh dikenakan tindakan tatatertib.

Tindakan: Semua

LAMPIRAN I

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MPB

Nama (Huruf Besar) :

No. Kad Pengenalan :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

Tandatangan : _____

Tarikh : _____

Pengesahan Pegawai Keselamatan ICT MPB

_____
( )

Pegawai Keselamatan ICT (ICTSO)
Lembaga Lada Malaysia

b.p. Ketua Pengarah MPB
Tarikh :

LAMPIRAN II

ARAHAN KEPADA PEKHIDMAT, KONTRAKTOR DAN PIHAK KETIGA

Selaras dengan pematuhan Dasar Keselamatan ICT di MPB, tuan/ puan hendaklah mematuhi peraturan keselamatan ICT yang telah ditetapkan. Pelanggaran kepada dasar ini boleh menyebabkan perkhidmatan/ bekalan tuan/ puan dihentikan serta-merta dan dikenakan penalti sewajarnya. Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

a) Mendapatkan kebenaran daripada MPB untuk menjalankan aktiviti perkhidmatan / bekalan dengan memaklumkan tarikh, masa dan bilangan pekerja yang terlibat. Semua pembekal bertanggungjawab memastikan pekerja adalah bebas jenayah.
b) Menyatakan dengan lengkap dan jelas skop kerja/ bekalan/ perkhidmatan yang akan dijalankan.
c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.
d) Bilik Server dan bilik/ruang yang terdapat peralatan ICT kritikal/kabel telekomunikasi (MDF room/riser).adalah kawasan larangan ICT dan kebenaran hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. Pembekal adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi tujuan tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan hendaklah diiringi pegawai yang dibenarkan sepanjang masa sehingga tugas di kawasan berkenaan selesai.
e) Kawasan penghantaran barangan dan *loading area* hendaklah dikawal/ dipantau dan perlu dipisahkan dari akses terus ke kawasan larangan.

SURAT AKUAN PEMATUHAN BAGI
PEKHIDMAT, KONTRAKTOR DAN PIHAK KETIGA
DASAR KESELAMATAN ICT MPB

Nama (Huruf Besar) :

No. Kad Pengenalan :

Jawatan :

Syarikat :

Skop Kerja :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan - peruntukan yang terkandung di dalam Dasar Keselamatan ICT MPB.

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : _____

Tarikh : _____