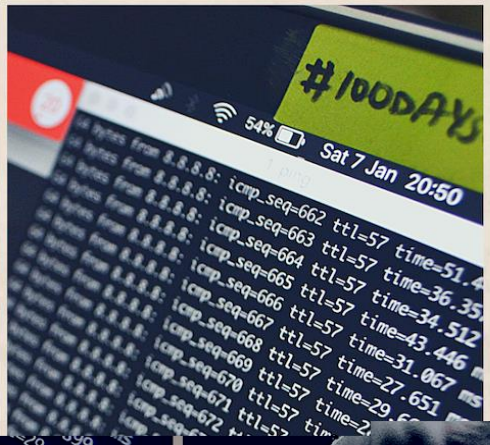
KEMENTERIAN PENDIDIKAN MALAYSIA



POLISI

ESELAMATAN SIBER

KE

KEMENTERIAN PENDIDIKAN MALAYSIA

Versi 1.0

SEJARAH DOKUMEN

TARIKH	VERSI	PEKELILING	TARIKH KUATKUASA
16 April 2019	1.0	ICT BIL 1 TAHUN 2019	30 April 2019

KANDUNGAN

PENGENALAN **11**

OBJEKTIF **11**

PENYATAAN DASAR **12**

SKOP **13**

PRINSIP-PRINSIP **15**

PENILAIAN RISIKO KESELAMATAN ICT **17**

BIDANG 01: POLISI KESELAMATAN MAKLUMAT **18**

0101 Polisi Keselamatan Maklumat **19**

010101 Pelaksanaan Polisi 19

010102 Penyebaran Polisi 19

010103 Penyelenggaraan Polisi 19

010104 Pengecualian Polisi 19

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT **20**

0201 Infrastruktur Keselamatan Organisasi **21**

020101 Ketua Setiausaha 21

020102 Ketua Pegawai Maklumat (CIO) 21

020103 Pegawai Keselamatan ICT (ICTSO) 22

020104 Pengurus/Penyelaras ICT 23

020105 Pentadbir Sistem ICT 23

020106 Pentadbir Pusat Data 24

020107 Pentadbir Rangkaian ICT 24

020108 Pegawai Aset 24

020109 Pengguna 25

0202 Pihak Ketiga **27**

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga 27

BIDANG 03: KESELAMATAN SUMBER MANUSIA **28**

0301 Keselamatan Sumber Manusia Dalam Tugas Harian **29**

030101 Sebelum Perkhidmatan 29

030102 Dalam Perkhidmatan 29

030103 Bertukar Atau Tamat Perkhidmatan 30

KANDUNGAN

BIDANG 04: PENGURUSAN ASET 31

0401 Akauntabiliti Aset 32

040101 Inventori Aset 32

0402 Pengelasan dan Pengendalian Maklumat 33

040201 Pengelasan Maklumat 33

040202 Pengendalian Maklumat 33

BIDANG 05: KAWALAN CAPAIAN 34

0501 Dasar Kawalan Capaian 35

050101 Keperluan Kawalan Capaian 35

0502 Pengurusan Capaian Pengguna 36

050201 Akaun Pengguna 36

050202 Hak Capaian 36

050203 Pengurusan Kata Laluan 37

050204 *Clear Desk* dan *Clear Screen* 38

0503 Kawalan Capaian Rangkaian 39

050301 Capaian Rangkaian 39

050302 Capaian Internet 39

0504 Kawalan Capaian Sistem Pengoperasian 41

050401 Capaian Sistem Pengoperasian 41

0505 Kawalan Capaian Aplikasi dan Maklumat 42

050501 Capaian Aplikasi dan Maklumat 42

0506 Peralatan Mudah Alih dan Kerja Jarak Jauh 43

050601 Penggunaan Peralatan Mudah Alih 43

050602 Kerja Jarak Jauh 43

BIDANG 06: KAWALAN KRIPTOGRAFI 44

0601 Kawalan Kriptografi 45

060101 Enkripsi 45

KANDUNGAN

060102 Tandatangan Digital 45
060103 Pengurusan Infrastruktur Kunci Awam (PKI) 45
BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN 46
0701 Keselamatan Kawasan 47
070101 Kawalan Kawasan 47
070102 Kawalan Masuk Fizikal 48
070103 Kawasan Terperingkat 49
0702 Keselamatan Peralatan 50
070201 Peralatan ICT 50
070202 Media Storan 52
070203 Media Tandatangan Digital 53
070204 Media Perisian dan Aplikasi 53
070205 Penyelenggaraan Peralatan ICT 54
070206 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat 54
070207 Peralatan di Luar Premis 55
070208 Pelupusan Perkakasan 55
0703 Keselamatan Persekitaran 57
070301 Kawalan Persekitaran 57
070302 Bekalan Kuasa 58
070303 Kabel 58
070304 Prosedur Kecemasan 59
0704 Keselamatan Dokumen 60
070401 Dokumen 60
BIDANG 08: KESELAMATAN OPERASI 61
0801 Pengurusan Prosedur Operasi 62
080101 Pengendalian Prosedur 62
080102 Kawalan Perubahan 62
080103 Pengasingan Tugas dan Tanggungjawab 63
0802 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga 64
080201 Perkhidmatan Penyampaian 64

KANDUNGAN

0803 Perancangan dan Penerimaan Sistem 65

080301 Perancangan Kapasiti 65

080302 Penerimaan Sistem 65

0804 Perisian Berbahaya 66

080401 Perlindungan Dari Perisian Berbahaya 66

080402 Perlindungan daripada *Mobile Code* 66

0805 Housekeeping 67

080501 Sandaran (*Backup)* 67

0806 Pengurusan Media 68

080601 Penghantaran dan Pemindahan 68

080602 Pengurusan Media 68

080603 Keselamatan Sistem Dokumentasi 68

0807 Pemantauan 69

080701 Pengauditan dan Forensik ICT 69

080702 Jejak Audit 70

080703 Sistem Log 70

080704 Pemantauan Log 71

BIDANG 09: KESELAMATAN KOMUNIKASI 72

0901 Pengurusan Rangkaian 73

090101 Kawalan Infrastruktur Rangkaian 73

0902 Pengurusan Pertukaran Maklumat 75

090201 Pertukaran Maklumat 75

090202 Pengurusan Mel Elektronik 75

0903 Perkhidmatan Dalam Talian (*Online*) 77

090301 Perkhidmatan Dalam Talian (*Online*) 77

090302 Maklumat Umum 77

KANDUNGAN

0904 Media Sosial 78

090401 Media Sosial 78

090402 Keselamatan Media Sosial 78

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM 79

1001 Keselamatan Dalam Membangunkan Sistem dan Aplikasi 80

100101 Keperluan Keselamatan Sistem Maklumat 80

100102 Validasi Data *Input* dan *Output* 80

1002 Keselamatan Fail Sistem 81

100201 Kawalan Fail Sistem 81

1003 Keselamatan dalam Proses Pembangunan dan Proses Sokongan 82

100301 Prosedur Kawalan Perubahan 82

1004 Pembangunan Sistem Aplikasi 83

100401 Prosedur Pembangunan Sistem Aplikasi 83

100402 Pembangunan Perisian Secara *Outsource* 84

1005 Kawalan Teknikal Keterdedahan (*Vulnerability*) 85

100501 Kawalan dari Ancaman Teknikal 85

100502 Kawalan Kod Sumber dan Dokumentasi Sistem Aplikasi 85

1006 Pembangunan Laman Web 86

100601 Prosedur Pembangunan Laman Web 86

1007 Pembangunan Aplikasi Mudah Alih 87

100701 Prosedur Intergrasi Pembangunan Aplikasi Mudah Alih 87

BIDANG 11: HUBUNGAN PEMBEKAL 88

1101 Perolehan 89

110101 Pemilihan Syarikat Pembekal 89

110102 Kontrak 89

1102 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal 90

110201 Polisi Keselamatan Maklumat Ke Atas Pembekal 90

110202 Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal 90

110203 Kawalan Keselamatan Maklumat Dengan Pembekal Dan Pihak Ketiga 90

KANDUNGAN

1103 Pengurusan Penyampaian Perkhidmatan Pembekal 91

110301 Pemantauan dan Kajian Perkhidmatan Pembekal 91

110302 Pengurusan Perubahan Perkhidmatan Pembekal 91

BIDANG 12: RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT 92

1201 Mekanisme Pelaporan Insiden Keselamatan ICT 93

120101 Mekanisme Pelaporan 93

1202 Pengurusan Maklumat Insiden Keselamatan ICT 94

120201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT 94

BIDANG 13: KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN 95

1301 Dasar Kesinambungan Perkhidmatan 96

130101 Pelan Kesinambungan Perkhidmatan 96

130102 Mengesah, Mengkaji semula dan Menilai Keselamatan Maklumat dalam Pelan Pengurusan Kesinambungan Perkhidmatan 98

BIDANG 14: PEMATUHAN 99

1401 Pematuhan dan Keperluan Perundangan 100

140101 Pematuhan Dasar 100

140102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal 100

140103 Pematuhan Keperluan Audit 101

140104 Keperluan Perundangan 101

140105 Pelanggaran Dasar 101

140106 Privasi dan Perlindungan Maklumat Peribadi 101

140107 Hak Harta Intelek (*Intellectual Property Rights* - IPR) 102

1402 Kajian Keselamatan Maklumat 103

140201 Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat 103

140202 Pematuhan Kajian Teknikal 103

TERMA DAN TAFSIRAN 104

KANDUNGAN

LAMPIRAN 109
LAMPIRAN A 110
LAMPIRAN A1 111
LAMPIRAN B 112

PENGENALAN

Polisi Keselamatan Siber Kementerian Pendidikan Malaysia (KPM) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) KPM (termasuk Jabatan di bawahnya). Dasar ini juga menerangkan kepada semua pengguna di KPM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KPM.

OBJEKTIF

Polisi Keselamatan Siber KPM diwujudkan untuk menjamin kesinambungan urusan KPM dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama Keselamatan ICT KPM ialah seperti berikut:

a) Memastikan kelancaran operasi KPM 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;
c) Mencegah salah guna atau kecurian aset ICT Kerajaan;
d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan; dan
e) Memperkemaskan pengurusan keselamatan ICT KPM.

PENYATAAN DASAR

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

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

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

Polisi Keselamatan Siber KPM 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 KPM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Polisi Keselamatan Siber KPM menetapkan keperluan-keperluan asas berikut:

a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

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

a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KPM. 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 KPM;

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

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

d) Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif KPM. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod KPM, 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 KPM 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 Polisi Keselamatan Siber KPM dan perlu dipatuhi adalah seperti berikut:

a) Akses atas dasar perlu mengetahui

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

b) Hak akses minimum

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

c) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT;

d) Pengasingan

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

f) Pematuhan

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

g) Pemulihan

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

h) Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

KPM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu KPM perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat KPM termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

KPM bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. KPM perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

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

01

POLISI KESELAMATAN MAKLUMAT

0101 Polisi Keselamatan Maklumat

Objektif

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

010101 Pelaksanaan Polisi	Tanggungjawab
Pelaksanaan polisi ini akan dijalankan oleh Ketua Setiausaha KPM dibantu oleh Pasukan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pengarah Negeri, Pengurus/Penyelaras ICT, Pegawai Keselamatan ICT (ICTSO), dan semua Setiausaha/Pengarah Bahagian.	Ketua Setiausaha

010102 Penyebaran Polisi	Tanggungjawab
Polisi ini perlu disebar kepada semua pengguna KPM (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO

010103 Penyelenggaraan Polisi	Tanggungjawab
Piawaian berhubung dengan penyelenggaraan Polisi Keselamatan Siber KPM adalah seperti berikut: a. Polisi ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa bagi memastikan dokumen sentiasa dipatuhi; b. Mengemukakan cadangan pindaan secara bertulis, membuat pembentangan dan mendapatkan kelulusan pindaan daripada Jawatankuasa Pemandu ICT (JPICT) KPM; dan c. Memaklumkan perubahan yang telah dipersetujui oleh JPICT kepada semua pengguna.	ICTSO

010104 Pengecualian Polisi	Tanggungjawab
Polisi Keselamatan Siber KPM adalah terpakai kepada semua pengguna ICT KPM dan tiada pengecualian diberikan.	Pengguna dan Pihak Ketiga

02

ORGANISASI KESELAMATAN MAKLUMAT

0201 Infrastruktur Keselamatan Organisasi

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

020101 Ketua Setiausaha — Tanggungjawab

Ketua Setiausaha

Peranan dan tanggungjawab Ketua Setiausaha adalah seperti berikut:

a. Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber KPM dan semua jabatan/ agensi di bawahnya;
b. Memperuntukkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategi keselamatan Siber KPM dan semua jabatan/ agensi di bawahnya;
c. Memastikan semua pengguna mematuhi Polisi Keselamatan Siber KPM;
d. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KPM; dan
e. Melantik CIO dan ICTSO serta memaklumkan pelantikan kepada Ketua Pengarah MAMPU.

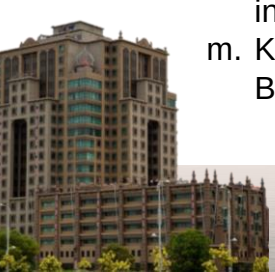
020102 Ketua Pegawai Maklumat (CIO) — Tanggungjawab

CIO

Timbalan Ketua Setiausaha (Pengurusan) KPM adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab CIO adalah seperti berikut:

a. Membantu Ketua Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;
b. Menentukan keperluan keselamatan ICT;
c. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan
d. Bertanggungjawab ke atas perkara-perkara yang berkaitan keselamatan ICT KPM.

020103 Pegawai Keselamatan ICT	Tanggungjawab
Pegawai Keselamatan ICT (ICTSO) yang dilantik adalah berperanan dan bertanggungjawab seperti berikut: a. Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan organisasi; b. Mengurus keseluruhan program-program keselamatan ICT KPM; c. Menguatkuasakan dan memantau pelaksanaan Polisi Keselamatan Siber KPM; d. Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber KPM kepada semua pengguna; e. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber KPM; f. Menjalankan tugas pengurusan risiko; g. Menjalankan audit, kajian semula, merumus tindak balas pengurusan KPM berdasarkan hasil penemuan dan menyediakan laporan mengenainya; h. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; i. Melaporkan insiden keselamatan ICT kepada Agensi Keselamatan Siber Negara (NACSA) dan memaklumkan kepada CIO; j. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; k. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; l. 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 m. Koordinator Pelan Pengurusan Pemulihan Bencana (DR Koordinator) KPM.	ICTSO



020104 Pengurus/Penyelaras ICT	Tanggungjawab
Pengurus/ Penyelaras ICT KPM adalah berperanan dan bertanggungjawab seperti berikut: a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KPM; b. Menentukan kawalan akses semua pengguna terhadap aset ICT KPM; c. Melaporkan penemuan mengenai pelanggaran Polisi Keselamatan Siber KPM kepada ICTSO; dan d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KPM.	Pengurus/ Penyelaras ICT

020105 Pentadbir Sistem ICT	Tanggungjawab
Pentadbir Sistem ICT KPM adalah berperanan dan bertanggungjawab seperti berikut:	

020109 Pengguna	Tanggungjawab

Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

Pengguna

a. Membaca, memahami, dan mematuhi Polisi Keselamatan Siber KPM;
b. Mengetahui dan memahami implikasi keselamatan ICT akibat daripada tindakannya;
c. Menjalani tapisan keselamatan seperti yang diarahkan (sekiranya berkaitan);
d. Melaksanakan dan mematuhi prinsip-prinsip Polisi Keselamatan Siber KPM serta menjaga kerahsiaan maklumat KPM;
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 Polisi Keselamatan Siber KPM sebagaimana **Lampiran A.**

0202 Pihak Ketiga

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

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	Tanggungjawab
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber KPM; 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 KPM perlu berlandaskan kepada perjanjian kontrak; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai; dan i) Polisi Keselamatan Siber KPM; ii) Tapisan Keselamatan; iii) Perakuan Akta Rahsia Rasmi 1972; dan iv) Hak Harta Intelek. f. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber KPM sebagaimana **Lampiran A-1.**	CIO, ICTSO, Pengurus/ Penyelaras ICT, Pentadbir Pusat Data, Pentadbir Sistem ICT, Pentadbir Rangkaian ICT, Pemilik Projek dan Pihak Ketiga

03

KESELAMATAN SUMBER MANUSIA

0301 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif :

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

030101 Sebelum Perkhidmatan	Tanggungjawab
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan KPM serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan KPM serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengguna dan Pengurusan Sumber Manusia

030102 Dalam Perkhidmatan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan Pengguna serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KPM;	Pengguna dan Pengurusan Sumber Manusia

030102 Dalam Perkhidmatan	Tanggungjawab
b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT KPM secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c. Memastikan adanya proses tindakan disiplin dan/ atau undang-undang ke atas pegawai dan kakitangan KPM serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh KPM; dan d. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Pengurusan Sumber Manusia, KPM.	Pengguna dan Pengurusan Sumber Manusia

030103 Bertukar Atau Tamat Perkhidmatan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua aset ICT dikembalikan kepada KPM mengikut peraturan dan/ atau terma perkhidmatan yang ditetapkan; dan b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh KPM.	Pengguna dan Pengurusan Sumber Manusia

04

PENGURUSAN ASET

0401 Akauntabiliti Aset

Objektif :
Memberi dan menyokong perlindungan yang bersesuaian ke atas pengguna aset ICT KPM.

040101 Inventori Aset	Tanggungjawab
Ini bertujuan memastikan pengguna aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan pengguna aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; b. Memastikan pengguna aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. Mengenal pasti lokasi pengguna aset ICT yang telah ditempatkan di KPM; d. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan e. Setiap pengguna adalah bertanggungjawab ke atas aset ICT di bawah kawalannya.	Pegawai Aset dan Pengguna

0402 Pengelasan dan Pengendalian Maklumat

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

040201 Pengelasan Maklumat	Tanggungjawab
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia besar; b. Rahsia; c. Sulit; atau d. Terhad.	Pengguna

040202 Pengendalian Maklumat	Tanggungjawab
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.	Pengguna

0501 Dasar Kawalan Capaian

Objektif :
Mengawal capaian ke atas maklumat.

050101 Keperluan Kawalan Capaian	Tanggungjawab
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.	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

0502 Pengurusan Capaian Pengguna

Objektif :
Mengawal capaian pengguna ke atas aset ICT KPM.

050201 Akaun Pengguna	Tanggungjawab
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh KPM sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan mencerminkan identiti pengguna; c. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan KPM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; d. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e. Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i) Bertukar bidang tugas kerja; ii) Bertukar ke agensi lain; iii) Bersara; atau iv) Ditamatkan perkhidmatan.	Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT dan Pengguna

050202 Hak Capaian	Tanggungjawab
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

050203 Pengurusan Kata Laluan	Tanggungjawab
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KPM seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; d. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; e. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; f. Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; g. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; h. Mengelakkan penggunaan semula kata laluan yang baru digunakan; dan i. Penetapan kata laluan hendaklah mematuhi kombinasi panjang kata laluan sekurang-kurangnya lapan (8) aksara dengan gabungan aksara dan angka.	Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT dan pengguna

050204 *Clear Desk* dan *Clear Screen*	Tanggungjawab
Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; b. Dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Pengguna

0503 Kawalan Capaian Rangkaian

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

050301 Capaian Rangkaian	Tanggungjawab
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian KPM, rangkaian agensi lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

050302 Capaian Internet	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di KPM hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian KPM; b. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus/ Penyelaras ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; c. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/ pegawai yang diberi kuasa;	Pengurus/ Penyelaras ICT, Pentadbir Sistem ICT, Pentadbir Rangkaian ICT dan pengguna

050302 Capaian Internet	Tanggungjawab
d. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; e. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan 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 KPM; dan h. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i) Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii) Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah, perjudian atau keganasan.	Pengurus/ Penyelaras ICT, Pentadbir Sistem ICT, Pentadbir Rangkaian ICT dan pengguna

0504 Kawalan Capaian Sistem Pengoperasian

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

050401 Capaian Sistem Pengoperasian	Tanggungjawab
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 c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c. Menghadkan dan mengawal penggunaan program; dan d. Menghadkan tempoh capaian (*session timed-out*) ke sesebuah aplikasi berisiko tinggi.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

0505 Kawalan Capaian Aplikasi dan Maklumat

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

050501 Capaian Aplikasi dan Maklumat	Tanggungjawab
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c. Setiap aktiviti capaian kepada sistem dan aplikasi yang berisiko tinggi hendaklah dihadkan kepada pengguna yang sah sahaja. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; 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.	Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT dan ICTSO

0506 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif :
Memastikan keselamatan maklumat apabila menggunakan peralatan mudah alih dan kerja jarak jauh.

050601 Penggunaan Peralatan Mudah Alih	Tanggungjawab
Perkara-perkara berikut hendaklah dipatuhi: a. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; dan b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua

050602 Kerja Jarak Jauh	Tanggungjawab
Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

06

KAWALAN KRIPTOGRAFI

0601 Kawalan Kriptografi

Objektif :
Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

060101 Enkripsi	Tanggungjawab
Pengguna hendaklah membuat enkripsi ke atas maklumat sensitif atau maklumat rahsia rasmi yang termaktub di dalam buku arahan keselamatan pada setiap masa.	Pengguna

060102 Tandatangan Digital	Tanggungjawab
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna berkaitan khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pengguna

060103 Pengurusan Infrastruktur Kunci Awam (PKI)	Tanggungjawab
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. Perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan sijil digital hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b. Sijil digital hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. Perkongsian sijil digital untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; dan d. Sebarang perubahan kepada pemilik atau kehilangan/kerosakan hendaklah dilaporkan kepada pentadbir sistem.	Pemilik Sistem dan Pentadbir Sistem ICT

07

KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Keselamatan Kawasan

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

070101 Kawalan Kawasan	Tanggungjawab
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c. Memasang alat penggera atau kamera; d. Mengehad jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan; h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan yang disediakan; j. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO

070101 Kawalan Kawasan	Tanggungjawab
l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO

070102 Kawalan Masuk Fizikal	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap kakitangan di KPM hendaklah memakai atau mengenakan kad ID Jabatan sepanjang waktu bertugas; b. Semua kad ID Jabatan hendaklah diserahkan balik kepada KPM apabila pengguna berhenti atau bersara; c. Setiap pelawat perlu mendaftar dan mendapatkan pas pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; d. Kehilangan pas pelawat mestilah dilaporkan dengan segera kepada Pengawal Keselamatan; dan e. Hanya kakitangan dan pelawat yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT tertentu KPM.	Pengguna dan Pelawat

070103 Kawasan Terperingkat	Tanggungjawab
Kawasan terperingkat ditakrifan sebagai kawasan yang menempatkan aset ICT berisiko tinggi dan meliputi kawasan premis atau sebahagian daripada premis di mana rahsia rasmi disimpan, diuruskan atau di mana kerja terperingkat dijalankan. Akses ke kawasan terperingkat adalah dihadkan dengan kebenaran. a. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan b. Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	Pejabat Ketua Pegawai Keselamatan Kerajaan, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

0702 Keselamatan Peralatan

Objektif :
Melindungi peralatan ICT KPM daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

070201 Peralatan ICT	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian antivirus di komputer yang dipertanggungjawabkan kepada pengguna sentiasa aktif *(activated)* dan dikemas kini di samping melakukan imbasan ke atas media storan luaran yang digunakan; g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h. Peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); i. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; j. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;	Pengguna

070201 Peralatan ICT	Tanggungjawab
k. Peralatan ICT yang hendak dibawa keluar dari premis KPM, perlulah mendapat kebenaran bertulis dari Pentadbir Sistem ICT dan direkodkan seperti yang dinyatakan dalam pekeliling perbendaharaan sedia ada bagi tujuan pemantauan;	Pengguna
l. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera mengikut pekeliling perbendaharaan sedia ada;	
m. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;	
n. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;	
o. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih;	
p. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;	
q. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang telah ditetapkan;	
r. Pengguna dilarang sama sekali mengguna dan mengubah kata laluan akaun pentadbir (*administrator password*) pada komputer yang dipertanggungjawabkan dan telah ditetapkan;	
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. Semua pergerakan aset ICT KPM hendaklah direkodkan.	

070202 Media Storan	Tanggungjawab
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti CDROM, *thumb drive* dan media storan lain. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat: a. Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media adalah terhad kepada pegawai 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; e. Pergerakan media storan hendaklah direkodkan; f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; i. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; j. Menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja; dan k. Kitaran hayat data hendaklah diuruskan mengikut Akta Arkib Negara (Akta 629).	Pengguna

070203 Media Tandatangan Digital	Tanggungjawab
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 mengikut peraturan semasa yang ditetapkan.	Pengguna

070204 Media Perisian dan Aplikasi	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan KPM; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus/ Penyelaras ICT; c. Lesen perisian (*registration code, serials,* CD-*keys*) perlu disimpan berasingan daripada CDROM, *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.	Pengguna

070205 Penyelenggaraan Peralatan ICT	Tanggungjawab
Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. 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. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; e. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pentadbir ICT berkenaan; f. Semua aktiviti penyelenggaraan perlu direkodkan; dan g. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pengguna

070206 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat	Tanggungjawab
Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan: a. Peralatan yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai yang mengurus aset ICT dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Pengguna

070207 Peralatan Di Luar Premis	Tanggungjawab
Bagi perkakasan yang dibawa keluar dari premis KPM, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan KPM: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan; dan c. Kehilangan peralatan ICT perlu dilaporkan mengikut peraturan semasa yang ditetapkan.	Pengguna

070208 Pelupusan Perkakasan	Tanggungjawab
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KPM. Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KPM: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui kaedah: i) penyingkiran (*purging*) seperti *secure erase* atau *degaussing;* atau ii) pemusnahan media secara fizikal (*destroying*) seperti penghancuran (*disintegration*), kisaran halus (*pulverization*), peleburan dan pembakaran. b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c. Peralatan ICT yang akan dilupuskan hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupus atau sebaliknya;	Pegawai Aset

070208 Pelupusan Perkakasan	Tanggungjawab
e. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT;	Pegawai Aset
f. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;	
g. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;	
h. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *external hard disk* atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; dan	
i. Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:	
i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;	
ii) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hard disk*, *motherboard* dan sebagainya;	
iii) Menyimpan dan memindahkan perkakasan luaran komputer seperti *Automatic Voltage Regulator (AVR), speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di KPM;	
iv) Memindah keluar dari KPM mana-mana peralatan ICT yang hendak dilupuskan; dan	
v) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab KPM.	

0703 Keselamatan Persekitaran

Objektif :
Melindungi aset ICT KPM dari sebarang bentuk acaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

070301 Kawalan Persekitaran	Tanggungjawab
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubah suai, pembelian hendaklah mematuhi garis panduan, tatacara dan prosedur yang sedang berkuatkuasa. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pengesan kebakaran, alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Semua bahan mudah terbakar, cecair bahan atau peralatan lain yang boleh merosakkan peralatan ICT, hendaklah diletakkan di tempat yang bersesuaian dan berjauhan daripada aset ICT; e. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT; dan f. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya sekali dalam setahun atau mengikut keperluan. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	Pegawai Keselamatan, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

070302 Bekalan Kuasa	Tanggungjawab
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi daripada kegagalan bekalan elektrik dan bekalan yang sesuai. b. Peralatan sokongan seperti UPS *(Uninterruptable Power Supply)* dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa, diuji dan diselenggara secara berjadual.	Pegawai Keselamatan, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

070303 Kabel	Tanggungjawab
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pegawai Keselamatan, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

070304 Prosedur Kecemasan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan yang sedang berkuatkuasa; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan.	Pegawai Keselamatan dan Pengguna

0704 Keselamatan Dokumen

Objektif :
Melindungi maklumat KPM daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, pencerobohan, kemalangan atau kecurian.

070401 Dokumen	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap dokumen hendaklah difailkan 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 seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan e. Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Pengguna

08

KESELAMATAN OPERASI

0801 Pengurusan Prosedur Operasi

Objektif :
Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.

080101 Pengendalian Prosedur	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, 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; c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan; dan d. Semua kakitangan KPM hendaklah mematuhi prosedur yang telah ditetapkan.	Pengguna

080102 Kawalan Perubahan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Pengurus/ Penyelaras ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh Juruteknik Komputer KPM atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Pengurus/ Penyelaras ICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

080102 Kawalan Perubahan	Tanggungjawab
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.	Pengurus/ Penyelaras ICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

080103 Pengasingan Tugas dan Tanggungjawab	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesah data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan c. Aset ICT yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari aset ICT yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus/ Penyelaras ICT dan Pentadbir Sistem ICT

0802 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

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

080201 Perkhidmatan Penyampaian	Tanggungjawab
Perkara-perkara yang perlu 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 secara berkala; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua

0803 Perancangan dan Penerimaan Sistem

Objektif :
Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

080301 Perancangan Kapasiti	Tanggungjawab
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO dan Pentadbir Sistem ICT

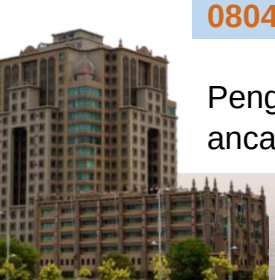
080302 Penerimaan Sistem	Tanggungjawab
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pengurus/ Penyelaras ICT, ICTSO dan Pentadbir Sistem ICT

0804 Perisian Berbahaya

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

080401 Perlindungan Dari Perisian Berbahaya	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d. Mengemaskini *pattern* antivirus yang terkini; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Melaksanakan dan menghadiri program kesedaran mengenai acaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Semua

080402 Perlindungan daripada *Mobile Code*	Tanggungjawab
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua



0805 *Housekeeping*

Objektif :
Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.

080501 Sandaran (*Backup*)	Tanggungjawab
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Perkara–perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi baharu; b. Membuat salinan sandaran ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan penduaan bergantung kepada tahap kritikal maklumat; c. Menguji sistem sandaran dan prosedur *restore* yang sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d. Melaksanakan sandaran secara harian, mingguan, bulanan dan tahunan bergantung kepada tahap kritikal maklumat; dan e. Merekod dan menyimpan salinan sandaran di lokasi yang berlainan dan selamat.	Pentadbir Pusat Data

0806 Pengurusan Media

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

080601 Penghantaran dan Pemindahan	Tanggungjawab
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua

080602 Pengurusan Media	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan; 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 hendaklah dihapus atau dimusnahkan mengikut prosedur yang ditetapkan.	Semua

080603 Keselamatan Sistem Dokumentasi	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Semua

0807 Pemantauan

Objektif :
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

080701 Pengauditan dan Forensik ICT	Tanggungjawab
Bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT KPM; b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; h. Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT; dan i. Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

080702 Jejak Audit	Tanggungjawab
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod setiap aktiviti transaksi; b. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT

080703 Sistem Log	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti 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. Melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

080704 Pemantauan Log	Tanggungjawab
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. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubah suai dan sebarang capaian yang tidak dibenarkan; c. Aktiviti pentadbiran dan operator sistem perlu direkodkan; d. Kesalahan, kesilapan dan/ atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan e. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KPM atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

09

KESELAMATAN KOMUNIKASI

0901 Pengurusan Rangkaian

Objektif :
Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

090101 Kawalan Infrastruktur Rangkaian	Tanggungjawab
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; *d.* *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat terperingkat Kerajaan serta dikonfigurasi sendiri oleh pentadbir sistem dan perlu mengambil kira perkara-perkara berikut: i. Sebarang permohonan buka/tutup port perlu dimaklumkan secara rasmi untuk tujuan pengrekodan; ii. Semua aliran trafik (*multimedia* dan data) daripada dalam ke luar KPM dan sebaliknya mestilah melalui *firewall;* iii. Hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya berasaskan kepada Polisi Keselamatan Siber KPM dan Perjanjian Perkhidmatan Rangkaian WAN/PCN bersama pihak MAMPU; dan iv. Reka bentuk *firewall* hendaklah mengambilkira perkara berikut: • Keperluan audit dan arkib; • Kebolehsediaan; • Kerahsiaan; dan • Melindungi maklumat KPM.	Pentadbir Rangkaian ICT dan Pentadbir Sistem ICT

090101 Kawalan Infrastruktur Rangkaian	Tanggungjawab
e. Semua sistem aplikasi berasaskan web hendaklah diletakkan di dalam zon DMZ (*demilitarized zone*), manakala pangkalan data ditempatkan di *secured zone*; f. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; g. Sebarang penyambungan rangkaian yang bukan di bawah kawalan KPM hendaklah mendapat kebenaran ICTSO; h. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum; i. Sebarang penyambungan rangkaian daripada pihak ketiga (*remote tunneling*) ke dalam sistem rangkaian KPM hendaklah mendapat kebenaran ICTSO; j. Capaian rangkaian Pusat Data hanya dihadkan melalui nod atau alamat IP yang dibenarkan sahaja; k. Pengawalan keperluan capaian peralatan melalui konfigurasi VLAN yang telah ditetapkan; l. Menyahaktifkan hebahan (*broadcast*); dan m. Kerja-kerja berkaitan rangkaian hanya boleh dilaksanakan oleh kakitangan yang terlatih dan dibenarkan sahaja.	Pentadbir Rangkaian ICT dan Pentadbir Sistem ICT

0902 Pengurusan Pertukaran Maklumat

Objektif :
Memastikan keselamatan pertukaran maklumat dan perisian antara KPM dan agensi luar terjamin.

090201 Pertukaran Maklumat	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mewujudkan prosedur kawalan pertukaran maklumat yang formal untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KPM; dan c. Melindungi sebaik-baiknya maklumat yang terdapat di dalam media.	Semua

090202 Pengurusan Mel Elektronik	Tanggungjawab
Penggunaan mel elektronik (emel) di KPM hendaklah dipantau secara berterusan oleh Pentadbir emel untuk memenuhi keperluan etika penggunaan emel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam oleh Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan” dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengunakan akaun atau alamat emel yang diperuntukkan oleh KPM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Setiap emel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh KPM; c. Pengguna hendaklah mengelak dari membuka emel daripada penghantar yang tidak diketahui atau diragui;	Semua

090202 Pengurusan Mel Elektronik	Tanggungjawab
d. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui emel; e. Setiap emel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; f. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; g. Mengambil tindakan dan memberi maklum balas terhadap emel dengan cepat serta mengambil tindakan segera; dan h. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	Semua

0903 Perkhidmatan Dalam Talian (*Online*)

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

090301 Perkhidmatan Dalam Talian (*Online*)	Tanggungjawab

Bagi menggalakkan pertumbuhan perkhidmatan dalam talian serta sebagai menyokong hasrat kerajaan mengoptimumkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet.

Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Maklumat yang terlibat dalam transaksi dalam talian perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;
b. Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan
c. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

090302 Maklumat Umum	Tanggungjawab

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

Pengguna

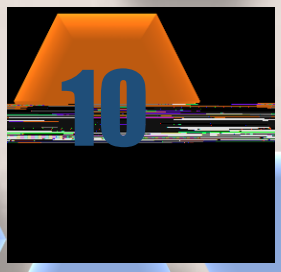
a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;
b. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan
c. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.

0904 Media Sosial

Objektif :
Memastikan keselamatan dan kawalan penyebaran maklumat melalui media sosial.

090401 Media Sosial	Tanggungjawab
Perkara-perkara yang perlu dipatuhi di dalam memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi dan disebarkan melalui media sosial adalah seperti berikut: a. Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara; b. Tidak melibatkan penyebaran maklumat dan dokumen terperingkat; c. Tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan; d. Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; dan e. Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan.	Semua

090402 Keselamatan Media Sosial	Tanggungjawab
Pegawai yang bertanggungjawab mengendalikan laman web media sosial rasmi perlulah memastikan keselamatan media sosial dengan melaporkan masalah *spam* kepada Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM).	Pentadbir Sistem ICT



PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

1001 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

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

100101 Keperluan Keselamatan Sistem Maklumat	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna serta 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.	Pentadbir Sistem ICT

100102 Validasi Data *Input* dan *Output*	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b. Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT

1002 Keselamatan Fail Sistem

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

100201 Kawalan Fail Sistem	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian; dan d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal.	Pemilik Sistem dan Pentadbir Sistem ICT

1003 Keselamatan dalam Proses Pembangunan dan Proses Sokongan

Objektif :
Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

100301 Prosedur Kawalan Perubahan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum digunapakai; b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pembangun sistem yang dibenarkan sahaja; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	Pentadbir Sistem ICT

1004 Pembangunan Sistem Aplikasi

Objektif :
Memastikan pembangunan sistem aplikasi secara *in-house* dan *outsource* perlu diselia dan dipantau untuk memastikan ia mengikut jadual dan prosedur yang telah ditetapkan.

100401 Prosedur Pembangunan Sistem Aplikasi	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pembangunan sistem aplikasi hendaklah mengambil kira sistem aplikasi sedia ada di KPM dan agensi lain bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama; b. Sesuatu pembangunan sistem aplikasi perlu mempunyai pemilik sistem kepada sistem aplikasi tersebut; c. Pemilik Sistem aplikasi bertanggungjawab mempromosi dan memastikan kelancaran pelaksanaan sistem; d. Pemilik Sistem aplikasi hendaklah membaca dan memahami dokumentasi serta mematuhi prosedur yang berkaitan; e. Memastikan pembangunan sistem menggunakan teknik *secure coding*; f. Setiap sistem, aplikasi dan perisian hendaklah mematuhi garis panduan keselamatan dan lulus *User Acceptance Test* (UAT) dan *Final Acceptance Test* (FAT); dan g. Setiap sistem perlu mendapatkan pengesahan daripada JPICT sebelum dilancarkan.	Pemilik Sistem dan Pentadbir Sistem ICT

100402 Pembangunan Perisian Secara *Outsource*	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua spesifikasi perolehan dan kontrak komersial hendaklah mengandungi keperluan mandatori seperti yang berikut: “Kod sumber, data/maklumat, prosedur dan dokumen adalah hak milik Kerajaan.”; b. Bagi sistem yang dibangunkan, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori seperti yang berikut: “Kerajaan berhak mencapai kod sumber dan data/maklumat” dan “Kerajaan berhak melaksanakan pengolahan risiko ke atas perisian yang dibangunkan.”; c. Perolehan produk tempatan atau yang dibangun menggunakan teknologi tempatan hendaklah diberi keutamaan dalam pembangunan dan keseluruhan kitar hayat sistem. Kakitangan dan sumber berkaitan sistem hendaklah dipilih untuk mengurangkan kebergantungan kepada sumber luaran, kepakaran dan teknologi asing; d. Setiap sistem, aplikasi dan perisian hendaklah mematuhi garis panduan keselamatan dan lulus *User Acceptance Test (UAT)* dan *Final Acceptance Test (FAT)*; e. Setiap sistem perlu mendapatkan pengesahan daripada JPICT sebelum dilancarkan; dan f. Penilaian keselamatan perlu dilakukan oleh pihak ketiga untuk memastikan keselamatan sistem.	Pemilik Sistem dan Pentadbir Sistem ICT

1005 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Objektif :
Memastikan kawalan teknikal keterdedahan (*vulnerability*) adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

100501 Kawalan dari Ancaman Teknikal	Tanggungjawab
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke	

11

HUBUNGAN PEMBEKAL

1101 Perolehan

Objektif :
Menerangkan perkara yang perlu dipatuhi dalam proses perolehan ICT.

110101 Pemilihan Syarikat Pembekal	Tanggungjawab
Pemilihan syarikat pembekal hendaklah mengikut peraturan seperti berikut: a. Memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b. Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; c. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; d. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; dan e. Jawatankuasa penilaian teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal.	Semua

110102 Kontrak	Tanggungjawab
Menyedia dan menyemak kontrak dengan menyediakan terma dan syarat yang bersesuaian bagi memastikan aktiviti KPM yang dilaksanakan mengikut undang-undang dan peraturan.	Pemilik Projek dan Penasihat Undang-undang

1102 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal

Objektif :
Memastikan aset ICT KPM yang boleh dicapai oleh pembekal dilindungi.

110201 Polisi Keselamatan Maklumat Ke Atas Pembekal	Tanggungjawab
Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa. Perkara–perkara yang perlu dipatuhi adalah seperti berikut: a. Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas; b. Pengurusan pembekal adalah tertakluk kepada peraturan yang sedang berkuat kuasa; c. Pengawalan dan pemantauan akses pembekal; dan d. Keperluan minimum keselamatan maklumat bagi setiap pembekal seperti keperluan perundangan atau pekeliling berkaitan hendaklah dinyatakan dalam perjanjian.	Pengurus/ Penyelaras ICT dan Pembekal

110202 Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal	Tanggungjawab
Semua keperluan keselamatan maklumat yang relevan hendaklah ditentukan dan dipatuhi oleh pembekal bagi tujuan mengakses, memproses, menyimpan, berkomunikasi dan menyediakan komponen infrastruktur ICT KPM. Perkara-perkara berikut hendaklah dipatuhi: a. Penerangan maklumat keselamatan; b. Keperluan undang-undang dan peraturan; dan c. Tapisan keselamatan pembekal.	Pengurus/ Penyelaras ICT dan Pembekal

110203 Kawalan Keselamatan Maklumat Dengan Pembekal Dan Pihak Ketiga	Tanggungjawab
Perjanjian dengan pembekal hendaklah meliputi risiko keselamatan yang merangkumi perkhidmatan ICT dengan pihak ketiga.	Pengurus/ Penyelaras ICT dan Pembekal

1103 Pengurusan Penyampaian Perkhidmatan Pembekal

Objektif :
Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan penyampaian perkhidmatan adalah sama seperti perjanjian pembekal.

110301 Pemantauan dan Kajian Perkhidmatan Pembekal	Tanggungjawab
KPM hendaklah sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal. Perkara-perkara berikut hendaklah dipatuhi: a. Pemantauan tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan; dan b. Laporan perkhidmatan yang dihasilkan oleh pembekal hendaklah dipantau dan status kemajuan dikemukakan kepada KPM.	Pemilik Projek

110302 Pengurusan Perubahan Perkhidmatan Pembekal	Tanggungjawab
Semua perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut *Standard Operating Procedure (SOP)* yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Perubahan dalam perjanjian dengan pembekal; b. Perubahan yang dilakukan oleh KPM bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c. Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pentadbir Sistem

12

RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

1201 Mekanisme Pelaporan Insiden Keselamatan ICT

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

120101 Mekanisme Pelaporan	Tanggungjawab
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 Polisi keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat.	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT dan CERT KPM

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO KPM dan Pasukan CERT KPM dengan kadar segera:

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

Pelaporan insiden keselamatan ICT di KPM sepertimana Prosedur pelaporan insiden keselamatan ICT berdasarkan:

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

1202 Pengurusan Maklumat Insiden Keselamatan ICT

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

120201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	Tanggungjawab
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 KPM. 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 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.	CERT KPM

13

KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1301 Dasar Kesinambungan Perkhidmatan

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

130101 Pelan Kesinambungan Perkhidmatan	Tanggungjawab
Pihak KPM hendaklah memastikan aspek keselamatan Maklumat dalam Pelan Kesinambungan Perkhidmatan (PKP) hendaklah dibangunkan, laksanakan dan dikemas kini (proses, prosedur serta kawalan) 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 Ketua Jabatan dan 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 di- persetujui; e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; f. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	Koordinator PKP KPM

130101 Pelan Kesinambungan Perkhidmatan	Tanggungjawab

PKP perlu dibangunkan dan hendaklah mengandungi

1401 Pematuhan dan Keperluan Perundangan

Objektif :
Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Polisi Keselamatan Siber KPM.

140101 Pematuhan Dasar	Tanggungjawab
Setiap pengguna di KPM hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber KPM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di KPM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT KPM selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber KPM. Tertakluk kepada pematuhan dasar yang dinyatakan ia hendaklah berasaskan keupayaan sebenar persekitaran yang boleh dilaksanakan melalui analisa jurang (*gap analysis*) tanpa menjejaskan objektif polisi.	Pengguna

140102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	Tanggungjawab
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO

140103 Pematuhan Keperluan Audit	Tanggungjawab
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.	Pengguna

140104 Keperluan Perundangan	Tanggungjawab
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di KPM adalah seperti di **Lampiran B**.	Pengguna

140105 Pelanggaran Dasar	Tanggungjawab
Pelanggaran Polisi Keselamatan Siber KPM boleh dikenakan tindakan tatatertib.	Pengguna

140106 Privasi dan Perlindungan Maklumat Peribadi	Tanggungjawab
KPM hendaklah mengenal pasti privasi dan perlindungan maklumat peribadi pengguna dijamin seperti yang tertakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan.	Pengguna

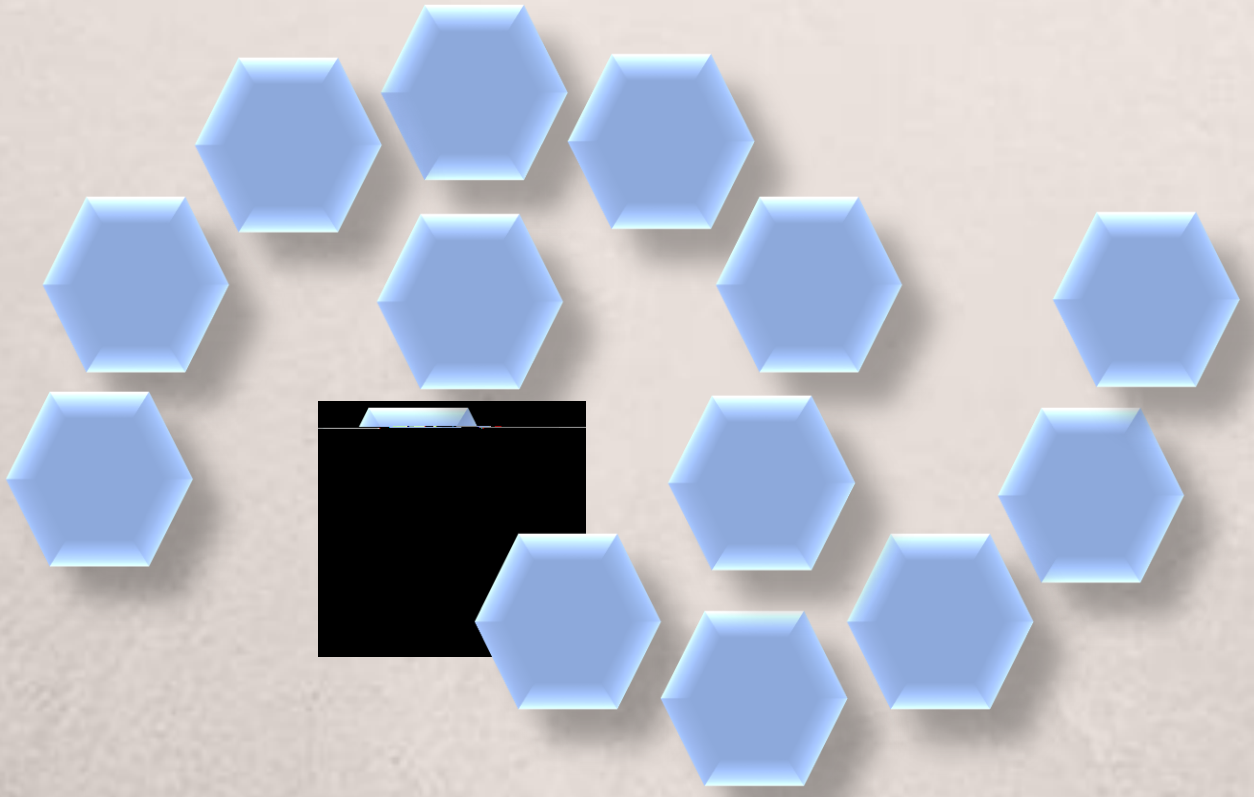
140107	Hak Harta Intelek (*Intellectual Property Rights* - IPR)	Tanggungjawab
	Prosedur-prosedur yang sesuai akan dilaksanakan untuk memastikan keselarasan dengan perundangan, peraturan dan juga keperluan kontrak yang berkaitan dengan *Intellectual Property Rights (IPR)* dan juga pelesenan perisian. KPM akan mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. Perkara-perkara berikut hendaklah dipatuhi: a. Pematuhan terhadap hak cipta yang berkaitan dengan perisian proprietari, dan reka bentuk yang diperoleh daripada KPM; b. Pematuhan terhadap perlesenan menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperoleh daripada KPM; dan c. Pematuhan terhadap hakcipta produk dan keperluan perlesenan.	Pengguna

1402 Kajian Keselamatan Maklumat

Objektif :
Memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur KPM.

140201 Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat	Tanggungjawab
Dalam pelaksanaan keselamatan maklumat KPM, kesemua prosedur, polisi dan proses keselamatan maklumat hendaklah disemak apabila terdapat perubahan ketara berlaku dalam pelaksanaannya.	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT

140202 Pematuhan Kajian Teknikal	Tanggungjawab
Sistem maklumat hendaklah sentiasa dikaji supaya selaras dengan pematuhan polisi dan standard keselamatan maklumat KPM (seperti *Security Posture Assessment – SPA*).	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian ICT



TERMA DAN TAFSIRAN

Terma dan Tafsiran

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, *pita magnetic, optical disk, flash disk*, CDROM dan *thumb drive* untuk sebarang kemungkinan adanya virus.
Ancaman	Apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab KPM.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur - Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CERT	*Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. CERT ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di KPM dan agensi di bawah KPM.
CIO	*Chief Information Officer* - Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.

Terma dan Tafsiran

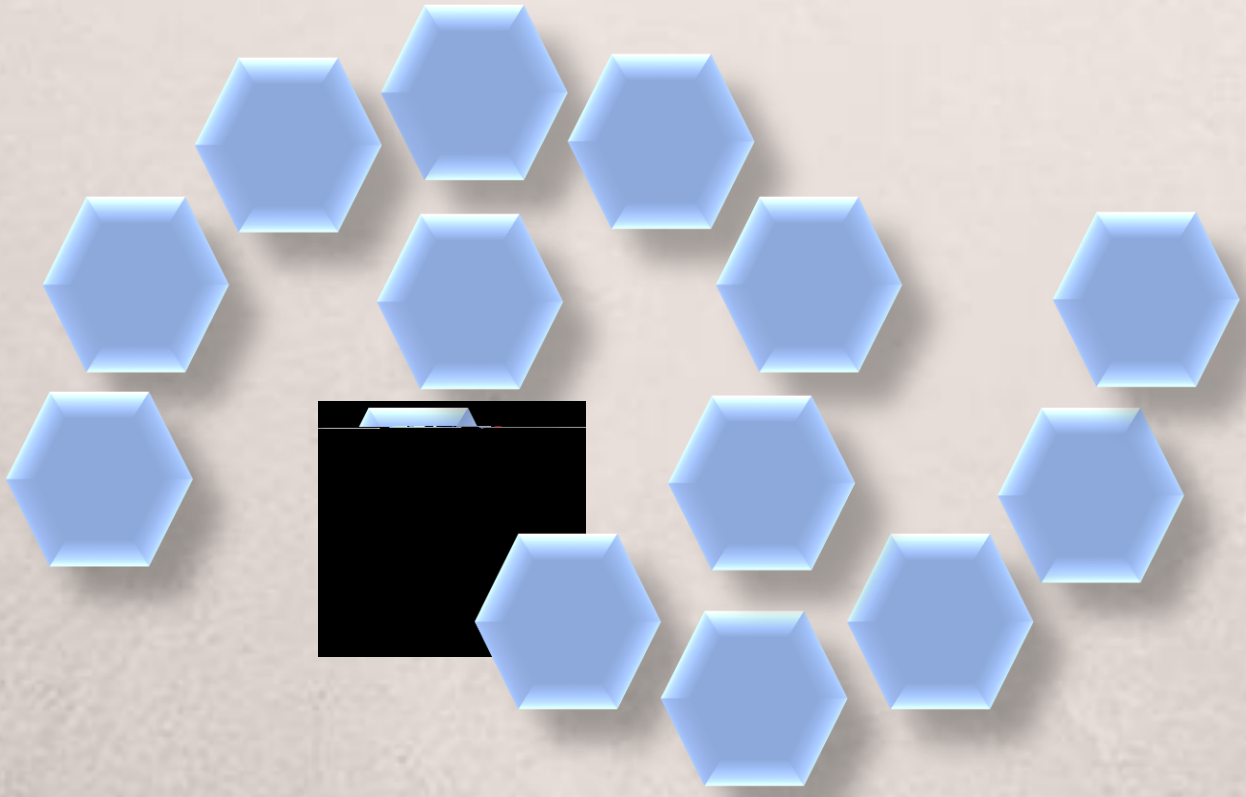
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft / espionage*), penipuan (*hoaxes*).
Hard disk	Cakera keras - Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	ICT *Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Intrusion Detection Sistem (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention Sistem (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus, trojan horse, worm, spyware* dan sebagainya.

Terma dan Tafsiran

Mobile code	Kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Keselamatan	Termasuk pegawai yang dilantik sebagai Pegawai Keselamatan Kerajaan atau mana-mana pegawai yang berkhidmat sebagai Pegawai Keselamatan Kerajaan atau pegawai yang menjalankan tugas sebagai Pegawai Keselamatan Kerajaan.
Pemilik Projek	Pemilik projek adalah pegawai yang mengurus dan memantau sesuatu projek ICT.
Pengurus Projek	Takrifan pengurusan projek
Pemilik Sistem	Pemilik sistem (*business owner*) bagi sistem yang dibangun atau yang paling banyak memiliki data.
Pengguna	Kakitangan KPM, pembekal, pakar runding dan pihak-pihak lain yang dibenarkan.
Pengurus/ Penyelaras ICT	Pegawai yang mengetuai organisasi ICT di Bahagian/Jabatan/Agensi KPM
Pengurus Sumber Manusia	Pegawai yang bertanggungjawab dalam aspek pengurusan personel dan pembangunan sumber manusia
Penilaian Risiko	Penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
Pentadbir Pusat Data	Pentadbir yang mengurus dan menyelenggara Pusat Data KPM.
Pentadbir Rangkaian ICT	Pentadbir yang melaksana dan menyelenggara rangkaian ICT dan komunikasi ICT.
Pentadbir Sistem ICT	Pentadbir yang menyelenggarakan sistem aplikasi, laman web dan aplikasi mudah alih serta mengurus operasi/sokongan teknikal.

Terma dan Tafsiran

Peralatan ICT	Merujuk kepada semua perkakasan dan perisian ICT.
Perisian	Set atur cara komputer yang menjalankan sesuatu tugas pada sistem komputer. Terdapat tiga (3) jenis perisian iaitu sistem pengendali (contohnya: Linux dan Windows), sistem utiliti (contohnya: *Disk Cleanup* dan *Disk Defragmenter*) dan perisian aplikasi (contohnya: Microsoft Office dan Google Chrome).
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Perkakasan ICT	Merujuk kepada komponen dalaman peralatan ICT.
Pihak Ketiga	Pihak yang membekalkan perkhidmatan kepada KPM.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Restore	Proses penarikan semula data.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Switch	Alat yang boleh menapis (filter) dan memajukan (*forward*) isyarat paket data antara segmen rangkaian LAN.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dansurat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.



LAMPIRAN

LAMPIRAN A

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN PENDIDIKAN MALAYSIA

Nama (Huruf Besar) : .....
No. Kad Pengenalan: .....
Jawatan : .....
Bahagian / Jabatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan–peruntukan yang terkandung di dalam Polisi Keselamatan Siber KPM; dan

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

Tandatangan : .....
Tarikh : .....

Pengesahan Ketua Jabatan / Bahagian

.....
( )

Tarikh : .....

LAMPIRAN A-1

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN PENDIDIKAN MALAYSIA

Nama (Huruf Besar) : .....
No. Kad Pengenalan: .....
Jawatan : .....
Syarikat : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan–peruntukan yang terkandung di dalam Polisi Keselamatan Siber KPM;

2. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub dalam Polisi Keselamatan Siber KPM; dan

3. Sekiranya saya atau mana-mana individu yang mewakili syarikat ini didapati melanggar dasar yang telah ditetapkan, maka saya sebagai wakil syarikat bersetuju tindakan undang-undang boleh diambil ke atas sesiapa yang terlibat mengikut peruntukan-peruntukan undang-undang sedia ada yang sedang berkuatkuasa.

Tandatangan : .....
Tarikh : .....

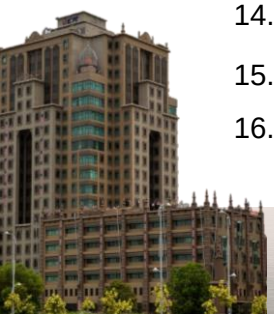
Pengesahan Ketua Jabatan / Bahagian

.....
( )

Tarikh : .....

Senarai Perundangan dan Peraturan

1. Arahan Keselamatan;
2. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
4. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
6. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
7. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
8. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
9. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
10. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksa- naan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
11. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
12. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
13. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
14. Akta Tandatangan Digital 1997;
15. Akta Rahsia Rasmi 1972;
16. Akta Jenayah Komputer 1997;



17. Akta Hak Cipta (Pindaan) Tahun 1997;
18. Akta Komunikasi dan Multimedia 1998;
19. Perintah-Perintah Am;
20. Arahan Perbendaharaan;
21. Arahan Teknologi Maklumat 2007;
22. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
23. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
24. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) April 2016, versi 1.0; dan
25. Akta-akta/Kaedah/Pekeliling/Arahan lain yang berkaitan.

Bahagian Pengurusan Maklumat
Kementerian Pendidikan Malaysia
Aras 3 & 4, Blok E11, Kompleks E
Pusat Pentadbiran Kerajaan Persekutuan
62604 Putrajaya