KEMENTERIAN PERTANIAN
DAN INDUSTRI ASAS TANI

POLISI KESELAMATAN SIBER

Versi 1.0

KANDUNGAN

SEJARAH DOKUMEN i

PENGENALAN ii

OBJEKTIF ii

PENYATAAN DASAR iii

SKOP iv

PRINSIP-PRINSIP vi

PENILAIAN RISIKO KESELAMATAN ICT viii

1. Polisi Keselamatan Maklumat 1

    1.1 Pelaksanaan Polisi 1

    1.2 Penyebaran Polisi 1

    1.3 Penyelenggaraan Polisi 1

    1.4 Pengecualian Polisi 1

2. Organisasi Keselamatan ICT 2

    2.1 Organisasi Keselamatan Maklumat 2

    2.2 Pihak Ketiga 7

    2.3 Peranti Mudah Alih dan *Teleworking* 8

3. KESELAMATAN SUMBER MANUSIA 9

    3.1 Sebelum Perkhidmatan 9

    3.2 Semasa Dalam Perkhidmatan 9

    3.3 Bertukar / Tamat Perkhidmatan 10

4. PENGURUSAN ASET 11

    4.1 Tanggungjawab terhadap Aset ICT 11

    4.2 Pengelasan, Pelabelan dan Pengendalian Maklumat 13

    4.3 Pengendalian Media Penyimpanan Maklumat 14

5. KAWALAN CAPAIAN 16
5.1 Pengurusan Kawalan Capaian 16
5.2 Pengurusan Capaian Pengguna 16
5.3 Kawalan Capaian Rangkaian 19
5.4 Kawalan Capaian Sistem dan Aplikasi 20
6. KRIPTOGRAFI 22
6.1 Enkripsi 22
6.2 Tandatangan Digital 22
6.3 Pengurusan Infrastruktur Kunci Awam (PKI) 22
7. KESELAMATAN FIZIKAL DAN PERSEKITARAN 23
7.1 Keselamatan Kawasan 23
7.2 Keselamatan Peralatan ICT 25
7.3 Keselamatan Persekitaran 32
7.4 Keselamatan Dokumen 35
8. KESELAMATAN OPERASI 36
8.1 Prosedur dan Tanggungjawab Operasi 36
8.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga 38
8.3 Perancangan dan Penerimaan Sistem 38
8.4 Perlindungan daripada Perisian Berbahaya 39
8.5 *Housekeeping* 40
8.6 Pengurusan Media 41
8.7 Pemantauan 42
9. KESELAMATAN KOMUNIKASI 45
9.1 Pengurusan Rangkaian 45
9.2 Pemindahan Maklumat 47
9.3 Perkhidmatan Dalam Talian (*Online*) 49
9.4 Media Sosial 50

10. PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM 51

10.1 Keperluan Keselamatan Sistem Maklumat 51

10.2 Keselamatan Dalam Proses Pembangunan dan Sokongan 53

11. HUBUNGAN PEMBEKAL 56

11.1 Keselamatan Maklumat dalam Hubungan Pembekal 56

11.2 Pengurusan Penyampaian Perkhidmatan Pembekal................................ 57

12. PENGURUSAN INSIDEN KESELAMATAN ICT 58

12.1 Pengurusan Insiden Dan Penambahbaikan Keselamatan Maklumat 58

13. KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN... 61

13.1 Pelan Kesinambungan Perkhidmatan (PKP) 61

13.2 Program Latihan dan Kesedaran Terhadap PKP...................................... 62

13.3 Pengujian PKP... 62

13.4 Ketersediaan Kemudahan Pemprosesan Maklumat................................. 63

14. PEMATUHAN... 64

14.1 Pematuhan Polisi... 64

14.2 Keperluan Perundangan... 64

14.3 Perlindungan dan Privasi Data Peribadi 64

14.4 Semakan Keselamatan Maklumat 64

14.5 Pelanggaran Perundangan... 65

14.6 Akuan Pematuhan Polisi Keselamatan Siber.. 65

14.7 Pematuhan Terhadap Hak Harta Intelek (*Intellectual Property Rights*) 65

TERMA DAN TAFSIRAN 66

LAMPIRAN A (i) 69

LAMPIRAN A (ii) 70

LAMPIRAN B 71

SEJARAH DOKUMEN

VERSI	KELULUSAN	TARIKH KUATKUASA
1.0	JPICT Bil. 3/2019	10 September 2019

PENGENALAN

Polisi Keselamatan Siber (PKS) Kementerian Pertanian dan Industri Asas Tani (MOA) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) MOA/Jabatan/Agensi di bawahnya dan juga menghuraikan pendekatan Kementerian dalam aspek keselamatan ICT. Dasar ini juga menerangkan kepada semua pengguna di MOA/Jabatan/Agensi di bawahnya mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MOA/Jabatan/Agensi.

OBJEKTIF

PKS MOA diwujudkan untuk menjamin kesinambungan urusan MOA dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama Keselamatan ICT MOA ialah seperti berikut:

a) Memastikan kelancaran operasi MOA 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 MOA.

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.

PKS MOA 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 sewenangwenangnya 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 MOA terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. PKS MOA menetapkan keperluan-keperluan asas berikut:

1) 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
2) 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, PKS MOA 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 MOA. 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 MOA;

c) Perkhidmatan

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

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

d) Data atau Maklumat

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

e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian MOA 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 sama ada di MOA atau mana-mana premis kerajaan atau swasta 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 PKS MOA dan perlu dipatuhi adalah seperti berikut:

a) Capaian atas dasar "perlu tahu"

Capaian terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu sahaja. Ini bermakna capaian 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 capaian minimum

Hak capaian pengguna hanya diberi pada tahap 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 capaian adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna;

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, segala aset ICT hendaklah ditentukan dapat menjana dan menyimpan log keselamatan dan jejak audit;

f) Pematuhan

PKS MOA 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

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

MOA 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 MOA 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.

MOA 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. MOA 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
d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

1. Polisi Keselamatan Maklumat

Objektif:

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

1.1 Pelaksanaan Polisi	Tanggungjawab
Pelaksanaan polisi ini akan dikuatkuasakan oleh Ketua Setiausaha MOA dan dilaksanakan oleh Pasukan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pengurus ICT, Pegawai Keselamatan ICT (ICTSO), dan semua Setiausaha/Pengarah Bahagian.	Ketua Setiausaha

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

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

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

2. Organisasi Keselamatan ICT

Objektif:

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

2.1 Organisasi Keselamatan Maklumat

2.1.1 Ketua Setiausaha / Ketua Jabatan

Peranan dan tanggungjawab Ketua Setiausaha / Ketua Jabatan adalah seperti berikut:

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

2.1.2 Ketua Pegawai Maklumat (CIO)

Peranan dan tanggungjawab CIO adalah seperti berikut:

a. Membantu Ketua Setiausaha / Ketua Jabatan 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 MOA.

2.1.3 Pegawai Keselamatan ICT

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 MOA;
c. Menguatkuasakan dan memantau pelaksanaan Polisi Keselamatan Siber MOA;
d. Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber MOA kepada semua pengguna;
e. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber MOA;
f. Menjalankan tugas pengurusan risiko;
g. Menjalankan audit, kajian semula, merumus tindak balas pengurusan MOA 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) MOA.

2.1.4 Pengurus ICT

Pengurus ICT adalah berperanan dan bertanggungjawab seperti berikut:

a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Kementerian/Jabatan/Agensi;
b. Menentukan kawalan akses semua pengguna terhadap aset ICT Kementerian/Jabatan/Agensi;
c. Melaporkan penemuan mengenai pelanggaran Polisi Keselamatan Siber MOA kepada ICTSO; dan
d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Kementerian/Jabatan/Agensi.

2.1.5 Pentadbir Sistem ICT

Pentadbir Sistem ICT adalah berperanan dan bertanggungjawab seperti berikut:

a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas;
b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber MOA;
c. Memantau aktiviti capaian harian pengguna;
d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;
e. Menyimpan dan menganalisis rekod jejak audit;
f. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; dan
g. Memastikan pembangunan sistem aplikasi mengambil kira dan mematuhi ciri-ciri keselamatan yang termaktub di dalam Polisi Keselamatan Siber MOA.

2.1.6 Pentadbir Rangkaian ICT

Pentadbir Rangkaian ICT adalah berperanan dan bertanggungjawab seperti berikut:

a. Memastikan rangkaian setempat (LAN), rangkaian luas (WAN) dan Wireless beroperasi sepanjang masa;
b. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;
c. memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian;
d. Mewartakan polisi dan garis panduan penggunaan rangkaian Kementerian/Jabatan/Agensi kepada pengguna; dan
e. melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (*Security Posture Assessment*, SPA) serta penilaian risiko keselamatan maklumat.

2.1.7 Pentadbir Pusat Data

Pentadbir Pusat Data adalah berperanan dan bertanggungjawab seperti berikut:

a) Memastikan persekitaran fizikal, data dan sistem aplikasi berada dalam keadaan baik dan selamat;
b) Menjadual dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala;
c) Menyediakan Pelan Pemulihan Bencana (DRP) bagi memastikan kesinambungan perkhidmatan; dan
d) Memastikan pusat data sentiasa beroperasi mengikut polisi yang telah ditetapkan.

2.1.8 Pegawai Aset

Pegawai Aset Kementerian/Jabatan/Agensi ialah pegawai yang dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab Pegawai Aset adalah seperti berikut:

a. Memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan;

b. Memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik secara bertulis oleh Ketua Jabatan/ Bahagian;
c. Memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset;
d. Memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan bertulis daripada Ketua Jabatan/Bahagian;
e. Memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ penaiktarafan aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira;
f. Memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama Kementerian/Jabatan/Agensi berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan;
g. Memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan;
h. Memastikan senarai daftar induk aset ICT Kerajaan disediakan;
i. Memastikan senarai aset ICT Kerajaan disediakan mengikut lokasi dan format Senarai Aset ICT Kerajaan dalam dua (2) salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset dan satu (1) salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi;
j. Memastikan setiap kerosakan aset ICT Kerajaan dilaporkan;
k. Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan;
l. Merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurangkurangnya sekali setahun; dan
m. Memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.

2.1.9 Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

a. Membaca, memahami, dan mematuhi Polisi Keselamatan Siber MOA;
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 MOA serta menjaga kerahsiaan maklumat Kementerian/Jabatan/Agensi;
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 MOA sebagaimana **Lampiran A**.

2.2 Pihak Ketiga

2.2.1 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 MOA; 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 Kementerian/Jabatan/Agensi perlu berlandaskan kepada perjanjian kontrak;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian ICT, Pemilik Projek dan Pihak Ketiga

e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai; i. Polisi Keselamatan Siber MOA; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. f. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber MOA sebagaimana **Lampiran A(ii)**.	

2.3 Peranti Mudah Alih dan *Teleworking*

2.3.1 Peranti mudah alih milik persendirian

Peranti mudah alih milik persendirian hendaklah dikawal daripada mencapai maklumat Rahsia Rasmi dan hendaklah mematuhi polisi serta prosedur yang ditetapkan untuk dibawa masuk ke kawasan terperingkat.

2.3.2 *Teleworking*

i. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;

ii. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan

iii. Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk peralatan mudah alih dan alatan komunikasi.

3. KESELAMATAN SUMBER MANUSIA

Objektif:

Memastikan semua pihak yang terlibat dalam pengurusan dan penggunaan ICT memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dan kesedaran dalam aspek keselamatan ICT bagi mengurangkan risiko kecurian, penipuan dan penyalahgunaan aset ICT.

3.1 Sebelum Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menjelaskan peranan dan tanggungjawab pihak yang terlibat dalam meningkatkan keselamatan penyampaian maklumat dan mengurangkan risiko penyalahgunaan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pihak yang terlibat selaras dengan keperluan perkhidmatan, mengikut peraturan sedia ada; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani.	ICTSO/ Pengurus ICT/ Pengurus Sumber Manusia/ Pengguna
3.2 Semasa Dalam Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan pihak terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT secara berterusan dalam	Pengguna dan Pengurusan Sumber Manusia

melaksanakan tugastugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c) Memastikan tindakan disiplin atau undang-undang dilaksanakan sekiranya berlaku pelanggaran peraturan yang ditetapkan; 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, MOA/Jabatan/Agensi.	
3.3 Bertukar / Tamat Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua aset ICT dikembalikan kepada Kementerian/Jabatan/Agensi mengikut peraturan dan atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.	ICTSO/ Pentadbir Sistem ICT/ Pegawai Aset/ Pengguna

4. PENGURUSAN ASET

Objektif:

Memastikan setiap aset hendaklah dikenal pasti, dikelas, direkod dan di selenggara untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT.

4.1 Tanggungjawab terhadap Aset ICT

4.1.1 Inventori dan Pemilikan Aset ICT	Tanggungjawab
Semua aset ICT di Kementerian/Jabatan/Agensi mestilah diuruskan mengikut peraturan dan tatacara yang berkuat kuasa seperti berikut: a) Setiap aset ICT hendaklah didaftarkan dan ditentukan pemiliknya. b) Pemilik aset hendaklah menentukan klasifikasi keselamatan yang bersesuaian bagi setiap maklumat aset dan menentukan individu yang dibenarkan untuk capaian serta penggunaan maklumat tersebut; c) Pentadbir aset ICT adalah bertanggungjawab untuk menentukan prosedur kawalan khas (contohnya: kawalan capaian), kaedah pelaksanaan dan penyelenggaraan serta menyediakan langkah pemulihan yang konsisten dengan arahan pemilik aset; d) Semua pengguna aset ICT mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh pemilik aset atau pentadbir sistem. e) Kehilangan/ kecurian aset ICT mestilah dilaporkan serta merta mengikut prosedur pengurusan kehilangan/ kecurian aset berpandukan Arahan Perbendaharaan yang telah ditetapkan;	Pegawai Pengawal/ Pegawai Aset / Pentadbir Aset ICT/ Pemilik Aset/ Pengguna Aset

f) Setiap pengguna adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan aset ICT di bawah tanggungannya.	
4.1.2 Peralatan Mudah Alih dan Kerja Jarak Jauh	**Tanggungjawab**
Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti berikut: a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; c) Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT; d) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan e) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Pegawai Pengawal/ Pentadbir Aset ICT/ Pemilik Aset/ Pengguna Aset
4.1.3 Peminjaman dan Pemulangan Aset ICT	**Tanggungjawab**
<u>Peminjaman</u> Langkah-langkah yang perlu diambil termasuklah seperti berikut: a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh Kementerian/Jabatan/Agensi	Pegawai Pengawal/Pentadbir Aset ICT/Pemilik Aset/Pengguna Aset

bagi membawa keluar peralatan bagi tujuan yang dibenarkan; b) Melindungi dan mengawal peralatan sepanjang masa; c) Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan d) Menyemak peralatan ketika peminjaman dan pemulangan dilakukan. **Pemulangan** a) Memastikan semua aset ICT dikembalikan kepada Kementerian/Jabatan/Agensi mengikut peraturan dan atau terma perkhidmatan yang ditetapkan bagi pegawai yang: i. Bertukar keluar; ii. Bersara; iii. Ditamatkan perkhidmatan; dan iv. Diarahkan oleh Ketua Jabatan. b) Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.	

4.2 Pengelasan, Pelabelan dan Pengendalian Maklumat

4.2.1 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.	Pegawai Pengawal/ Pentadbir Aset ICT/ Pemilik Aset

4.2.2 Pelabelan dan Pengendalian Maklumat	Tanggungjawab
Semua maklumat mestilah dilabelkan mengikut klasifikasi maklumat seperti yang dinyatakan pada para 4.2.1 Pengelasan Maklumat. a) Aktiviti yang melibatkan pemprosesan maklumat seperti penyalinan, penyimpanan, penghantaran (sama ada dari segi lisan, pos, faksimili dan mel elektronik) dan pemusnahan maklumat mestilah mengikut standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; dan b) Maklumat yang diklasifikasikan sebagai Rahsia Besar, Rahsia, Sulit dan Terhad perlu dilindungi daripada didedahkan kepada pihak ketiga atau awam. Pihak ketiga jika perlu boleh diberi kebenaran capaian maklumat Kementerian/Jabatan/Agensi atas dasar perlu tahu sahaja dan mestilah mendapat kebenaran daripada Kementerian/Jabatan/Agensi.	Pentadbir Aset ICT/ Pemilik Aset

4.3 Pengendalian Media Penyimpanan Maklumat

4.3.1 Pengurusan Media	Tanggungjawab
a) Memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan aset secara tidak sah dan yang boleh mengganggu aktiviti perkhidmatan; b) Prosedur perlu disediakan untuk pengurusan peralatan penyimpanan maklumat mudah alih; c) Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna; dan d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Pentadbir Aset/ Pemilik Aset / Pengguna

4.3.2 Pelupusan Media	Tanggungjawab
a) Peralatan penyimpanan maklumat yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan;	Pentadbir Aset
4.3.3 Pemindahan Media	**Tanggungjawab**
a) Polisi, prosedur dan kawalan pertukaran maklumat yang rasmi perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi dalam agensi dan mana-mana pihak terjamin; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara agensi dengan pihak luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari agensi;	Pentadbir Aset/ Pemilik Aset / Pengguna

5. KAWALAN CAPAIAN

Objektif:

Mengawal capaian ke atas maklumat, aset ICT, rangkaian dan sistem aplikasi.

5.1 Pengurusan Kawalan Capaian

5.1.1 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

5.2 Pengurusan Capaian Pengguna

5.2.1 Akaun Pengguna	Tanggungjawab
a) Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan. b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat;	Pentadbir Sistem ICT / Pengguna

c) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan d) 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	
5.2.2 Hak Capaian	**Tanggungjawab**
a) Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas; dan b) Sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan.	Pentadbir Sistem ICT / Pengguna
5.2.3 Pengurusan Kata Laluan	**Tanggungjawab**
a) Memastikan pengunaan ID pengguna dan kata laluan tidak dikongsi; b) Membenarkan pengguna menukar kata laluan sendiri; c) Menggunakan kata laluan yang berkualiti (sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, simbol dan angka); d) Mewajibkan pengguna menukar kata laluan apabila log masuk kali pertama; e) Menyimpan rekod bagi kata laluan terdahulu dan mengelakkan penggunaan kata laluan yang berulang; f) Tidak memaparkan kata laluan di skrin ketika log masuk;	Pentadbir Sistem ICT / Pentadbir Pusat Data/ Pentadbir Rangkaian / Pengguna

g) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; h) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; i) Menyimpan kata laluan di dalam fail yang berasingan dengan fail data aplikasi; dan j) Mewajibkan pengguna menukar kata laluan sekurang-kurangnya setiap tiga (3) bulan untuk ke semua sistem utama.	
5.2.4 *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

5.3 Kawalan Capaian Rangkaian

5.3.1 Capaian Rangkaian	**Tanggungjawab**
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan b) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Pentadbir Sistem ICT dan Pentadbir Rangkaian
5.3.2 Capaian Internet	**Tanggungjawab**
a) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet 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; b) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus 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; d) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;	Pengurus ICT, Pentadbir Sistem ICT, Pentadbir Rangkaian dan pengguna

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; dan g) Pengguna adalah dilarang melakukan 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.	

5.4 Kawalan Capaian Sistem dan Aplikasi

5.4.1 Capaian Sistem Pengoperasian	**Tanggungjawab**
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) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan d) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. e) Menghadkan dan mengawal penggunaan program; dan	Pentadbir Sistem ICT dan Pentadbir Rangkaian

f) Menghadkan tempoh capaian (*session timed out*) ke sesebuah aplikasi berisiko tinggi.	
5.4.2 Capaian Sistem dan Aplikasi	**Tanggungjawab**
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. d) Mengehadkan capaian sistem dan aplikasi kepada lima (5) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; e) Menamatkan sesuatu sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan; f) Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem maklumat terperingkat (sulit/ rahsia); g) Pengguna digalakkan membuat enkripsi dengan menukarkan teks biasa (*plain text*) kepada bentuk *cipher text* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa; dan h) Capaian sistem dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem ICT, Pentadbir Rangkaian dan Pengguna

6. KRIPTOGRAFI

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

6.1 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
6.2 Tandatangan Digital	**Tanggungjawab**
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna berkaitan khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pengguna
6.3 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

7. KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif:

Memastikan maklumat, premis dan kemudahan ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang bentuk pencerobohan, ancaman, bencana alam, kerosakan, kecuaian serta akses yang tidak dibenarkan.

7.1 Keselamatan Kawasan

7.1.1 Keselamatan Fizikal	Tanggungjawab
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh premis. Langkah-langkah keselamatan fizikal adalah seperti 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) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan dan kunci harus disimpan oleh pegawai bertanggungjawab; c) Memperkukuhkan dinding dan siling; d) Memasang alat penggera dan sistem CCTV; e) Menghadkan jalan keluar masuk; f) Mengadakan kaunter kawalan; g) Menyediakan tempat atau bilik khas untuk pelawat; h) Mewujudkan perkhidmatan kawalan keselamatan; i) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang mendapat kebenaran sahaja untuk masuk; j) Merekabentuk dan melaksanakan perlindungan fizikal daripada bencana seperti kebakaran, banjir, letupan atau huru hara;	CGSO/ Pegawai Keselamatan/ CIO/ ICTSO

k) Menyediakan garis panduan keselamatan untuk kakitangan yang bekerja di dalam kawasan terhad; l) Sistem kawalan kunci dengan menetapkan pegawai yang bertanggungjawab untuk menyimpan kunci dengan baik dan mempunyai rekod; dan m) Mewujudkan kawalan di kawasan penghantaran, pemunggahan dan kawasan larangan.	
7.1.2 Kawalan Masuk Fizikal	**Tanggungjawab**
a) Setiap pengguna hendaklah memakai pas keselamatan sepanjang waktu bertugas; b) Setiap pelawat mestilah mendaftar dan mendapatkan pas pelawat di pintu masuk utama Kementerian/Jabatan/Agensi untuk ke kawasan/tempat berurusan dan hendaklah dikembalikan semula selepas tamat urusan; c) Semua pas keselamatan hendaklah diserahkan semula kepada Kementerian/Jabatan/Agensi apabila pengguna bertukar, berhenti atau bersara; dan d) Kehilangan pas keselamatan mestilah dilaporkan dengan segera kepada pegawai keselamatan Kementerian/Jabatan/Agensi.	Pengguna / Pelawat
7.1.3 Kawasan Larangan	**Tanggungjawab**
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di Kementerian/Jabatan/Agensi seperti di Pusat Data dan Bilik Fail. a) Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja;	ICTSO/ Pentadbir Rangkaian / Pentadbir Pusat Data / Pengguna/ Pihak Ketiga/ Pelawat

b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mendapat kebenaran untuk temujanji. Mereka hendaklah diiringi sepanjang masa sehingga tugas atau temujanji di kawasan berkenaan selesai; c) Semua aktiviti pihak ketiga di kawasan larangan perlu mendapat kebenaran daripada pegawai yang diberi kuasa dan dipantau serta dikawal oleh pegawai bertanggungjawab; d) Peralatan/ media perakaman/ storan/ komunikasi adalah tidak dibenarkan dibawa masuk ke dalam pusat data; dan e) Aktiviti mengambil gambar, merakam video, merekodkan suara atau penggunaan peralatan yang tidak berkenaan adalah dilarang.	

7.2 Keselamatan Peralatan ICT

7.2.1 Peralatan ICT	Tanggungjawab
Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan dengan mengambil tindakan berikut: a) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; b) Pengguna mesti mendapat kebenaran daripada pegawai yang diberikan kuasa untuk membuat instalasi perisian tambahan; c) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif dan	Pengguna/ Pentabir Sistem / Pihak Ketiga/ ICTSO/ pegawai aset

dikemaskini disamping melakukan imbasan ke atas media storan yang digunakan; d) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; e) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); f) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; g) Peralatan ICT yang hendak dibawa keluar dari premis Kementerian/Jabatan/Agensi untuk tujuan rasmi, perlu mendapat kelulusan pegawai yang diberikan kuasa dan direkodkan bagi tujuan pemantauan; h) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; i) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; j) Pengguna mesti mendapat kebenaran daripada pegawai yang diberikan kuasa untuk mengubah kedudukan komputer dari tempat asal; k) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada pegawai yang bertanggungjawab untuk dibaik pulih; l) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem; m) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang telah ditetapkan; n) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan	

hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; o) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat; p) Memastikan plug dicabut daripada suis bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya; q) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation)* yang sesuai. r) Memastikan semua aset ICT dikembalikan kepada mengikut peraturan dan terma yang ditetapkan; dan s) Membatalkan atau menarik balik semua kebenaran, capaian ke atas aset ICT mengikut peraturan yang ditetapkan.	
7.2.2 Media Storan	**Tanggungjawab**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, *thumb drive*, *external drive* dan media storan lain. Media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Tindakan berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan adalah terjamin dan selamat:	Pengguna/ Pentadbir Sistem ICT

a) Sediakan ruang penyimpanan yang kondusif dan selamat serta 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) Merekodkan pergerakan media storan untuk tujuan pinjaman; e) Mendapat kelulusan pemilik maklumat terlebih dahulu sebelum menghapuskan maklumat atau kandungan media storan dengan teratur dan selamat; f) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h) Perkakasan penduaan (*backup*) hendaklah diletakkan di tempat yang terkawal; dan i) Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan.	
7.2.3 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;	Pengguna/ Pentadbir Sistem ICT

b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan mengikut peraturan semasa yang ditetapkan.	
7.2.4 Media Perisian dan Aplikasi	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Kementerian/Jabatan/Agensi; b) Sistem aplikasi dalaman tidak dibenarkan dibentangkan atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c) Lesen perisian (*registration code*, *CD-keys* dan nombor siri) perlu disimpan berasingan daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	ICTSO/ Pentabir Sistem / Pengguna
7.2.5 Penyelenggaraan Peralatan ICT	**Tanggungjawab**
Peralatan ICT hendaklah diselenggarakan dengan baik bagi memastikan kerahsiaan, integriti dan kebolehsediaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;	Pengguna/ Pentabir Sistem ICT/ Pihak Ketiga

d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan e) Memaklumkan pengguna sebelum pelaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
7.2.6 Pinjaman Peralatan ICT	**Tanggungjawab**
Peralatan ICT yang dipinjam adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mendapatkan kelulusan mengikut peraturan dibawah Pekeliling Perbendaharaan Tatacara Pengurusan Aset atau peraturan Kementerian/Jabatan/Agensi bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; b) Pengguna hendaklah memohon peminjaman peralatan ICT melalui pegawai yang diberi kuasa; c) Pengguna perlu melindungi dan mengawal peralatan sepanjang tempoh pinjaman; d) Memastikan aktiviti pinjaman dan pemulangan peralatan ICT direkodkan; dan e) Memastikan peralatan ICT yang dipulangkan dalam keadaan baik dan lengkap.	Pengguna/ Pegawai Aset/ Pihak Ketiga
7.2.7 Peralatan ICT di Luar Premis	**Tanggungjawab**
Bagi peralatan ICT yang dibawa keluar dari premis, langkah-langkah keselamatan berikut hendaklah diambil: a) Peralatan ICT perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan	Pengguna/ Pegawai Aset/ Pengguna / Pihak ketiga

c) Memeriksa dan memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat Kerajaan. Maklumat perlu dihapuskan dari peralatan tersebut setelah disalin ke media storan sekunder.	
7.2.8 Pelupusan Peralatan Aset ICT	**Tanggungjawab**
Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa mengikut Tatacara Pengurusan Aset Alih Kerajaan. Pelupusan peralatan ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Kementerian/Jabatan/Agensi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua kandungan peralatan ICT khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilaksanakan 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 sebelum dipindahmilik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d) Butir-butir pelupusan hendaklah direkodkan dan dikemaskini; e) Pengguna adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;	Pegawai Aset, Pengguna

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

7.3 Keselamatan Persekitaran

7.3.1 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 peralatan komputer, 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;	ICTSO/ Bahagian Pentadbiran

<table>
<tr><td>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.
g) Akses kepada bilik sesalur telefon hendaklah sentiasa dikunci; dan
h) Mematuhi peraturan yang telah ditetapkan oleh pihak berkuasa seperti Jabatan Bomba dan Penyelamat, Jabatan Kerja Raya dan sebagainya.</td><td></td></tr>
<tr><td>7.3.2 Bekalan Kuasa</td><td>Tanggungjawab</td></tr>
<tr><td>Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:
a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan hendaklah disalurkan mengikut voltage yang bersesuaian;
b) Peralatan sokongan seperti Uninterruptable Power Supply (UPS) dan penjana (generator) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan
c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.</td><td>Pegawai Keselamatan/ ICTSO / Pentadbir Pusat Data dan Pentadbir Rangkaian</td></tr>
</table>

7.3.3 Kabel Peralatan ICT	Tanggungjawab
Kabel peralatan ICT hendaklah dilindungi kerana ia adalah salah satu punca maklumat. Langkah-langkah keselamatan kabel adalah seperti berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel dengan menggunakan konduit untuk mengelakkan 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
7.3.5 Prosedur Kecemasan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang telah ditetapkan; b) Melaporkan insiden kecemasan persekitaran kepada Pegawai Keselamatan; dan c) Mengadakan, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa.	ICTSO / Pengguna

7.4 Keselamatan Dokumen

7.4.1 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 ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Pengguna

8. KESELAMATAN OPERASI

Objektif:

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

8.1 Prosedur dan Tanggungjawab Operasi

8.1.1 Pengendalian Prosedur	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur operasi hendaklah didokumenkan dengan jelas, teratur, dikemaskinikan dan sedia diguna pakai oleh pengguna; b) Setiap perubahan kepada prosedur operasi mestilah dikawal; c) Tugas dan tanggungjawab fungsi perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset ICT; dan d) Kemudahan ICT untuk kerja-kerja pembangunan, pengujian dan operasi perlu diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.	ICTSO/ Pentadbir Sistem ICT
8.1.2 Pengurusan Perubahan	**Tanggungjawab**
Perubahan kepada organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang memberi kesan kepada keselamatan maklumat hendaklah dikawal. Pengurusan ke atas perubahan perlu diambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	ICTSO/Pengguna/ Pentadbir Sistem ICT

a) Mewujudkan prosedur pengurusan perubahan; b) Merekodkan semua perubahan yang telah dipersetujui dan dilaksanakan; dan c) Memantau pelaksanaan perubahan.	
8.1.3 Pengurusan Kapasiti	**Tanggungjawab**
Kapasiti sistem ICT hendaklah dirancang, diurus dan dikawal dengan terperinci bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan operasi sistem ICT. Keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO/ Pentadbir Sistem ICT
8.1.4 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi	**Tanggungjawab**
Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian ataupun perubahan tidak sah ke atas persekitaran operasi. Perkara–perkara yang perlu dipatuhi: a) Mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan operasi; b) Merekodkan semua penggunaan sumber yang dilaksanakan; dan c) Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.	ICTSO/ Pentadbir Sistem ICT

8.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

8.2.1 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

8.3 Perancangan dan Penerimaan Sistem

8.3.1 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

8.3.2 Penerimaan Sistem	Tanggungjawab
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Satu surat pengesahan penerimaan hendaklah dikeluarkan dengan persetujuan kedua-dua pihak.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

8.4 Perlindungan daripada Perisian Berbahaya

Objektif:

Memastikan aset ICT perlu dilindungi supaya tidak terdedah kepada kerosakan yang disebabkan oleh kod berbahaya seperti virus, worm, trojan dan lain-lain perisian berbahaya.

8.4.1 Perlindungan daripada Malware	Tanggungjawab
Perkara-perkara yang perlu dipatuhi bagi pencegahan, pengesanan dan pemulihan untuk melindungi sistem ICT daripada gangguan 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 manamana undang-undang bertulis yang berkuat kuasa; c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemaskini *pattern* antivirus yang terkini;	ICTSO/ Pentadbir Sistem ICT/ Pengguna

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; i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; j) Melaksanakan Program Kesedaran Pengguna yang bersesuaian; dan k) Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	

8.5 *Housekeeping*

Objektif:

Memastikan salinan pendua maklumat dan perisian sistem disediakan dan diuji secara berkala selaras dengan polisi pendua (*backup)* bagi tujuan kesinambungan operasi pemprosesan maklumat.

8.5.1 *Backup*	**Tanggungjawab**
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Membuat salinan pendua ke atas semua maklumat dan sistem perisian mengikut jadual yang ditetapkan atau apabila berlaku perubahan versi;	Pentadbir Pusat Data dan Pentadbir Sistem ICT

b) Menyimpan salinan pendua di lokasi lain yang selamat; dan c) Menguji sistem pendua bagi memastikan ianya dapat beroperasi dengan normal.	

8.6 Pengurusan Media

Objektif:

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

8.6.1 Penghantaran dan Pemindahan	**Tanggungjawab**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua
8.6.2 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) Menghadkan 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

8.6.3 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

8.7 Pemantauan

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan

8.7.1 Pengauditan dan Forensik ICT	Tanggungjawab
Bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a) Sebarang percubaan pencerobohan kepada sistem ICT; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan manamana pihak; d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;	ICTSO/ Pentadbir Sistem ICT/ Pentadbir Pusat Data /Pentadbir Rangkaian

f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; dan h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran.	
8.7.2 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 maklumatmaklumat 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

8.7.3 Sistem Log	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; a) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; b) Melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan. c) Semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; d) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubah suai dan sebarang capaian yang tidak dibenarkan; e) Aktiviti pentadbiran dan operator sistem perlu direkodkan; f) Kesalahan, kesilapan dan/ atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan g) Waktu yang berkaitan dengan sistem pemprosesan maklumat atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang piawai.	Pentadbir Sistem ICT / Pentadbir Pusat Data / Pentadbir Rangkaian

9. KESELAMATAN KOMUNIKASI

9.1 Pengurusan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

9.1.1 Kawalan Infrastruktur Rangkaian	**Tanggungjawab**
Infrastruktur rangkaian hendaklah dirancang, diurus dan dikawal bagi melindungi keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah: a) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berkaitan dengan sistem rangkaian; b) Peralatan keselamatan seperti *firewall* hendaklah dipasang bagi memastikan hak capaian ke atas sistem dapat dilaksanakan seperti ditetapkan; c) Sebarang cubaan menceroboh dan aktiviti yang boleh mengancam sistem dan maklumat Kementerian/Jabatan/Agensi perlu dipantau dan dikesan melalui pemasangan peralatan keselamatan seperti *Intrusion Prevention System* (IPS); d) Peralatan rangkaian hendaklah diletakkan di lokasi yang bebas dari risiko seperti banjir, gegaran dan habuk; e) Sebarang keperluan penyambungan rangkaian hendaklah melalui proses dan prosedur yang ditetapkan; f) Penggunaan rangkaian tanpa wayar (*wireless*) LAN di Kementerian/Jabatan/Agensi hendaklah mematuhi peraturan yang dikeluarkan oleh pihak berkenaan seperti MAMPU dan Majlis Keselamatan Negara (MKN); dan	ICTSO/ Pentadbir Rangkaian

g) Semua perisian berkaitan rangkaian dan keselamatan seperti *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.	
9.1.2 Keselamatan Perkhidmatan Rangkaian	**Tanggungjawab**
Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terjamin. Perkara-perkara yang perlu dipatuhi adalah: a) Mekanisme keselamatan, tahap kesediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara dalaman ataupun menggunakan sumber luar; b) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan di bawah kawalan Kementerian/Jabatan/Agensi; dan c) Sebarang aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam (PKPA) yang berkuat kuasa perlu disekat melalui penggunaan *Web Content Filtering*.	ICTSO / Pentadbir Rangkaian
9.1.3 Pengasingan Rangkaian	**Tanggungjawab**
Pengasingan perkhidmatan rangkaian bertujuan untuk meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara–perkara yang perlu dipatuhi adalah: a) Mengenal pasti fungsi dan tanggungjawab pengguna; b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan;	ICTSO / Pentadbir Rangkaian

c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Mengemaskinikan hak capaian pengguna dari masa ke semasa mengikut keperluan; dan e) Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	

9.2 Pemindahan Maklumat

9.2.1 Prosedur Pemindahan Maklumat	Tanggungjawab
Prosedur ini bertujuan untuk mengendali, menyimpan, memindah serta melindungi maklumat daripada didedah tanpa kebenaran atau salah guna serta memastikan keselamatan pemindahan maklumat dengan entiti luar terjamin. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menghadkan dan menentukan capaian kepada pengguna yang dibenarkan sahaja; b) Menghadkan pengedaran data untuk tujuan rasmi dan yang dibenarkan sahaja; c) Polisi, prosedur dan kawalan pemindahan maklumat yang formal perlu diwujudkan untuk melindungi pemindahan maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; d) Sebarang pemindahan maklumat di antara Kementerian/Jabatan/Agensi dan agensi lain mestilah dikawal; dan e) Penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi Kerajaan perlu mendapat kelulusan Ketua Jabatan; dan	ICTSO/ Pengguna/ Pentadbir Sistem ICT

f) Mewujudkan *Non-Disclosure Agreements* (NDA) bagi memastikan kerahsiaan, integriti dan ketersediaan (CIA) maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara Kementerian/Jabatan/Agensi dengan agensi luar.	
9.2.2 Pengurusan Mel Elektronik	**Tanggungjawab**
Penggunaan mel elektronik (emel) di MOA 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) Menggunakan akaun atau alamat emel yang diperuntukkan oleh Kementerian/Jabatan/Agensi sahaja. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b) Setiap emel yang disediakan hendaklah mematuhi format yang telah ditetapkan; c) Pengguna hendaklah mengelak dari membuka emel daripada penghantar yang tidak diketahui atau diragui; 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; dan	Pentadbir Emel / Pengguna

f) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	

9.3 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.

9.3.1 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. 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.	Pengguna

9.3.2 Maklumat Umum	Tanggungjawab
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Pengguna

9.4 Media Sosial

9.4.1 Keselamatan 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. f) 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).	Semua

10. PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

10.1 Keperluan Keselamatan Sistem Maklumat

Objektif:

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

10.1.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan; b) Semua sistem yang dibangunkan sama ada secara dalaman atau luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan berkaitan yang berkuat kuasa; dan c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan.	JK Penilaian Teknikal/ JPICT/ Pentadbir Sistem ICT/ Pembekal
10.1.2 Kawalan Keselamatan Sistem/Aplikasi di Rangkaian Awam	**Tanggungjawab**
Maklumat aplikasi yang menggunakan rangkaian awam hendaklah dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat, pengubahsuaian maklumat yang tidak dibenarkan yang menyebabkan pertikaian kontrak. Perkara-perkara yang perlu dipatuhi adalah:	Pengurus ICT/ Pentadbir Sistem ICT/Pembekal

a) Identiti pengguna perlu dikenal pasti dan disahkan bagi menentukan tahap capaian maklumat yang dibenarkan; b) Setiap pengguna sistem perlu diberi peranan mengikut skop dan tanggungjawab yang ditetapkan; dan c) Memastikan pembekal diberi penjelasan dan menandatangani akuan pematuhan PKS mengenai keperluan mematuhi kontrak dan peraturan keselamatan yang ditetapkan.	
10.1.3 Melindungi Transaksi Perkhidmatan Atas Talian	**Tanggungjawab**
Maklumat yang terlibat dalam transaksi perkhidmatan atas talian hendaklah dilindungi daripada penghantaran yang tidak lengkap, misrouting, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej.	Pengurus ICT, Pentadbir Sistem ICT
10.1.4 Validasi Data Input dan Output	**Tanggungjawab**
Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal. 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

10.2 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:

Memastikan keselamatan maklumat diwujudkan dan dilaksanakan dalam kitar hayat pembangunan sistem.

10.2.1 Polisi Keselamatan Dalam Pembangunan Sistem	**Tanggungjawab**
Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi dengan membangunkan Dokumen Pelan Pengurusan Keselamatan Maklumat (ISMP) semasa proses pembangunan sistem.	Pengurus ICT, Pentadbir Sistem ICT
10.2.2 Prosedur Kawalan Perubahan Sistem	**Tanggungjawab**
Prosedur kawalan perubahan hendaklah diwujudkan bagi mengawal sebarang perubahan terhadap sistem sepanjang kitar hayat pembangunan sistem. Perkara-perkara yang perlu dipatuhi adalah sepert berikut: a) Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang ditetapkan dan pelaksanaan hanya mengikut keperluan sahaja; b) Perubahan atau pengubahsuaian ke atas perisian dan sistem hendaklah diuji, didokumenkan dan disahkan sebelum diguna pakai; dan c) Setiap perubahan kepada pengoperasian sistem perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan maklumat.	Pengurus ICT, Pentadbir Sistem ICT, Pemilik Sistem
10.2.3 Semakan Teknikal Aplikasi Selepas Perubahan Platform	**Tanggungjawab**
Semakan dan pengujian terhadap aplikasi kritikal perlu dilaksanakan sekiranya berlaku perubahan terhadap platform pengoperasian bagi memastikan fungsi dan	Pentadbir Sistem ICT

operasi sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan sistem aplikasi, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan; dan b) Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan.	
10.2.4 Kawalan Terhadap Perubahan Kepada Perisian	**Tanggungjawab**
Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.	Pentadbir Sistem ICT
10.2.5 Prinsip Kejuruteraan Sistem Yang Selamat	**Tanggungjawab**
Prinsip kejuruteraan keselamatan sistem hendaklah dibangunkan, didokumenkan, dikaji dan digunapakai ke atas semua pelaksanaan sistem maklumat.	Pentadbir Sistem ICT
10.2.6 Persekitaran Pembangunan Sistem Yang Selamat	**Tanggungjawab**
Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem. Secara umumnya kitar hayat pembangunan sistem termasuk skop dan objektif sistem, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian, penerimaan, pemasangan, konfigurasi, penyelenggaraan dan pelupusan.	Pentadbir Sistem ICT
10.2.7 Pembangunan Sistem Secara Luaran	**Tanggungjawab**
Sebarang aktiviti pembangunan sistem yang melibatkan sumber luar perlu dikawal selia dan dipantau. Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut:	Pengurus ICT, Pentadbir Sistem ICT dan Pembekal

a) Memastikan spesifikasi perolehan mengandungi klausa tertentu berhubung keperluan keselamatan, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi Pasukan pembangunan; b) Organisasi hendaklah memastikan *Intellectual property rights* (IPR) dan kod sumber menjadi hak milik organisasi; c) Memasukkan klausa ke dalam kontrak yang membenarkan Kementerian/Jabatan/Agensi melaksanakan semakan terhadap kod sumber; dan d) Memasukkan klausa ke dalam kontrak yang membenarkan Kementerian/Jabatan/Agensi organisasi mendapat hak pemilikan kod sumber dan melaksanakan pengolahan risiko.	
10.2.8 Ujian Keselamatan Sistem	**Tanggungjawab**
Aktiviti pengujian penerimaan sistem hendaklah dilaksanakan ke atas sistem baru, naik taraf dan versi baru berdasarkan kriteria yang telah ditetapkan. Bagi memastikan integriti data, pengujian hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (*input*), peringkat pemprosesan data (*process*) dan peringkat penjanaan laporan (*output*).	Pengurus ICT dan Pentadbir Sistem ICT
10.2.9 Ujian Penerimaan Sistem	**Tanggungjawab**
Semua sistem baharu (termasuklah sistem yang dikemaskini/diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT dan Pemilik Sistem

11. HUBUNGAN PEMBEKAL

11.1 Keselamatan Maklumat dalam Hubungan Pembekal

Objektif :

Memastikan perkhidmatan yang diberi mempunyai tahap keselamatan ICT yang bersesuaian.

11.1.1 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 menandatangani Surat Akuan Pematuhan PKS MOA; b) Pembekal hendaklah menandatangani Akuan Akta Rahsia Rasmi 1972; c) Pembekal hendaklah menjalani ujian tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); dan d) Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas.	ICTSO/ Pembekal
11.1.2 Kawalan Keselamatan Maklumat Melalui Perjanjian dengan Pembekal	**Tanggungjawab**
Perjanjian dengan pihak pembekal hendaklah merangkumi keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan perkhidmatan teknologi maklumat dan komunikasi.	CIO, Pengurus ICT, dan Pembekal

11.1.3 Kawalan Keselamatan Maklumat Dengan Pembekal dan Pihak Ketiga	Tanggungjawab
Perjanjian dengan pembekal hendaklah meliputi risiko keselamatan yang merangkumi perkhidmatan ICT dan kesinambungan bekalan produk dengan pihak ketiga.	ICTSO, Pengurus ICT, Pembekal

11.2 Pengurusan Penyampaian Perkhidmatan Pembekal

Objektif :

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

11.2.1 Pemantauan dan Penilaian Perkhidmatan Pembekal	Tanggungjawab
Kementerian/Jabatan/Agensi hendaklah memantau, menyemak dan mengaudit perkhidmatan pembekal secara berkala.	Pemilik Projek / Pentadbir Sistem ICT
11.2.2 Pengurusan Perubahan Perkhidmatan Pembekal	**Tanggungjawab**
Setiap perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut SOP yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Perubahan di dalam perjanjian bersama pembekal; b) Perubahan yang dilakukan oleh Kementerian/Jabatan/Agensi 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.	Pengurus ICT / Pentadbir Sistem ICT

12. PENGURUSAN INSIDEN KESELAMATAN ICT

12.1 Pengurusan Insiden Dan Penambahbaikan Keselamatan Maklumat

Objektif:

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT supaya tidak menjejaskan imej MOA dan sistem penyampaian perkhidmatan..

12.1.1 Tanggungjawab Dan Prosedur	**Tanggungjawab**
Prosedur bagi mengurus insiden keselamatan ICT perlu diwujudkan dan didokumenkan. Kementerian/Jabatan/Agensi bertanggungjawab dalam pengurusan pengendalian insiden keselamatan ICT.	ICTSO / Pasukan CERT
12.1.2 Pelaporan Insiden Keselamatan Maklumat	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada Pasukan CERT. Semua maklumat adalah SULIT dan tidak boleh didedahkan tanpa kebenaran daripada ICTSO; b) Mematuhi prosedur operasi standard (SOP) keselamatan ICT Kementerian/Jabatan/Agensi; c) Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; d) Menyimpan jejak audit dan memelihara bahan bukti; dan e) Menyediakan dan melaksanakan pelan tindakan pemulihan.	Pasukan CERT

12.1.3 Pelaporan Kelemahan Keselamatan Maklumat	Tanggungjawab
Pelaporan juga perlu dilakukan sekiranya terdapat kelemahan keselamatan di dalam sistem atau perkhidmatan	Pasukan CERT / Pentadbir Sistem ICT/ Pentadbir Rangkaian / Pengguna
12.1.4 Penilaian dan Keputusan Insiden Keselamatan Maklumat	**Tanggungjawab**
Kejadian keselamatan maklumat perlu dinilai dan diklasifikasikan sebagai insiden keselamatan maklumat.	Pasukan CERT
12.1.5 Pengumpulan dan Pengendalian Bukti	**Tanggungjawab**
Maklumat mengenai insiden keselamatan ICT perlu dikumpul, dianalisis dan disimpan oleh Pengurus ICT bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan. Bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan bukti seperti jejak audit, backup berkala dan *off-site backup* hendaklah mengikut tatacara pengendalian yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Melindungi integriti bahan bukti; b) Mengumpul dan menyimpan bahan bukti bagi tujuan analisis; c) Merekodkan semua maklumat insiden termasuk maklumat pegawai yang terlibat, perisian, perkakasan dan peralatan yang digunakan; d) Memaklumkan kepada pihak berkuasa perundangan, seperti pegawai undang undang dan polis (jika perlu);	Pasukan CERT

e) Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang diperlukan (jika perlu); dan f) Menyediakan laporan insiden kepada CIO.	

13. KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif:

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

13.1 Pelan Kesinambungan Perkhidmatan (PKP)	Tanggungjawab
CIO hendaklah membangunkan Pelan Kesinambungan Perkhidmatan untuk mengekalkan kesinambungan perkhidmatan bagi memastikan tiada gangguan di dalam penyediaan perkhidmatan agensi. Pelan ini mestilah diperakui oleh pihak pengurusan Kementerian/Jabatan/Agensi dan perkara-perkara berikut perlu diberi perhatian: a) Melantik ahli Pasukan Pemulihan Bencana; b) Mengenal pasti dan mendokumenkan semua tanggungjawab dan prosedur kecemasan atau pemulihan; c) Melaksanakan prosedur-prosedur kecemasan dan simulasi pemulihan bencana bagi memastikan pemulihan dapat dilakukan dalam jangka masa yang telah ditetapkan seperti yang tertakluk dalam pelan pemulihan bencana; d) Mengadakan program kesedaran dan latihan kepada pengguna mengenai prosedur kecemasan; e) Mengkaji dan mengemas kini pelan sekurang-kurangnya setahun sekali; f) Membuat backup; dan g) Mewujudkan Pusat Pemulihan Bencana di lokasi lain.	Koordinator PKP

13.2 Program Latihan dan Kesedaran Terhadap PKP	Tanggungjawab
Semua kakitangan perlu mempunyai kesedaran dan mengetahui peranan masing-masing terhadap PKP. Ketua Jabatan bertanggungjawab dalam memastikan latihan dan program kesedaran terhadap PKP dilaksanakan setiap tahun.	Koordinator PKP

13.3 Pengujian PKP	Tanggungjawab
CIO perlu memastikan perkara-perkara berikut : a) PKP diuji dua (2) tahun sekali atau selepas perubahan utama, atau yang mana terdahulu bagi memastikan semua pihak yang berkenaan mengetahui dan maklum akan pelaksanaannya; b) Salinan PKP mestilah disimpan di lokasi berasingan bagi mengelakkan kerosakan akibat bencana di lokasi utama. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; c) Ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan; d) Kementerian/Jabatan/Agensi hendaklah memastikan salinan Pelan Kesinambungan Perkhidmatan sentiasa dikemas kini dan dilindungi seperti di lokasi utama; dan e) Komponen PKP seperti Pelan Pemulihan Bencana (*Disaster Recovery Plan* – DRP), Pelan Komunikasi Krisis (*Crisis Communication Plan* – CCP) dan Pelan Tindak Balas Kecemasan (*Emergency Response Plan* – ERP) perlu diuji dua (2) tahun sekali atau	Koordinator PKP

selepas perubahan utama, atau yang mana terdahulu.	
13.4 Ketersediaan Kemudahan Pemprosesan Maklumat	**Tanggungjawab**
Pasukan Pemulihan Bencana perlu memastikan semua sistem aplikasi dan perkakasan yang kritikal hendaklah mempunyai kemudahan redundancy dan diuji (*failover test*) keberkesanannya mengikut keperluan.	Pasukan Pemulihan Bencana

14. PEMATUHAN

Objektif:

Untuk menghindar pelanggaran undang-undang jenayah dan sivil, perlembagaan, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

14.1 Pematuhan Polisi
KSU adalah bertanggungjawab untuk memastikan bahawa pematuhan dan sebarang perlanggaran dielakan. Langkah-langkah perlu bagi mengelakkan sebarang perlanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Polisi Keselamatan Siber MOA dan undang-undang atau peraturanperaturan lain yang berkaitan yang berkuat kuasa.
14.2 Keperluan Perundangan
Kakitangan Kementerian/Jabatan/Agensi perlu memastikan senarai perundangan dan peraturan yang berkuat kuasa dari semasa ke semasa perlu dipatuhi oleh semua kakitangan di Kementerian/Jabatan/Agensi adalah seperti di **LAMPIRAN B**.
14.3 Perlindungan dan Privasi Data Peribadi
Privasi dan perlindungan maklumat peribadi pengguna dijamin seperti yang tertakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan.
14.4 Semakan Keselamatan Maklumat
Semakan keselamatan maklumat mestilah diambil kira seperti berikut: a) Pematuhan pemeriksaan ke atas PKS, piawaian dan prosedur perlu dilakukan secara tahunan. Pemeriksaan ini mestilah melibatkan usaha bagi menentukan kawalan yang mencukupi dan dipatuhi; b) Pengauditan perlu dilaksanakan sekurang-kurangnya sekali setahun terhadap pengoperasian sistem maklumat bagi meminimakan ancaman dan meningkatkan ketersediaan sistem; dan

c) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.

14.5 Pelanggaran Perundangan

Pelanggaran Polisi Keselamatan Siber MOA boleh dikenakan tindakan tatatertib.

14.6 Akuan Pematuhan Polisi Keselamatan Siber

KSU adalah bertanggungjawab untuk memastikan setiap pegawai menandatangani Akuan Pematuhan Polisi Keselamatan Siber seperti di **LAMPIRAN A (i)**.

14.7 Pematuhan Terhadap Hak Harta Intelek (*Intellectual Property Rights*)

ICTSO perlu memastikan prosedur pengawalan hendaklah dilaksanakan bagi memastikan pematuhan kepada perundangan, peraturan dan keperluan kontrak berkaitan produk yang mempunyai IPR termasuk perisian *proprietary*.

TERMA DAN TAFSIRAN

Antivirus	Perisian yang digunakan untuk mengesan dan membuang *malware*, seperti virus komputer, *adware*, *backdoors*, *malicious BHO's*, *dialers*, *fraudtools*, *hijackers*, *keyloggers*, *malicious LSPs*, *rootkits*, *spyware*, *trojan horses* dan *worms*.
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 di bawah tanggungjawab MOA.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
CERT	*Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT
Denial of service	Halangan pemberian perkhidmatan.
Enkripsi	Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan/pencurian identiti dan pencurian/penipuan maklumat.

Intrusion Detection System (IDS)	Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Perisian atau 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.
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.
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.
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.
Pemilik Sistem	Pemilik sistem (*business owner*) bagi sistem yang dibangun atau yang paling banyak memiliki data.
Pengguna	Kakitangan MOA, pembekal, pakar runding dan pihak-pihak lain yang dibenarkan.
Pengurus ICT	Pegawai yang mengetuai organisasi ICT di Kementerian/ Jabatan/ Agensi MOA.

Pentadbir Pusat Data	Pentadbir yang mengurus dan menyelenggara Pusat Data MOA.
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.
Pihak Ketiga	Pihak yang membekalkan perkhidmatan kepada MOA.
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.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan.

LAMPIRAN A (i)

AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN PERTANIAN DAN INDUSTRI ASAS TANI

Nama (Huruf Besar) : …………………………………………………………………..

No. Kad Pengenalan : ………………………………………………………………….

Jawatan : …………………………………………………………………...

Bahagian : ………………………………………………………………….

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

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

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

Tandatangan : …………………………….

Tarikh : …………………………….

Pengesahan Pegawai Keselamatan ICT

....
(Tandatangan & Cop Jawatan)

Tarikh: ....

* Polisi Keselamatan Siber boleh dicapai menerusi http://www.moa.gov.my

LAMPIRAN A (ii)

AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN PERTANIAN DAN INDUSTRI ASAS TANI

Nama (Huruf Besar) : …………………………………………………………………..

No. Kad Pengenalan : ………………………………………………………………….

Jawatan : ………………………………………………………………….....

Nama 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; dan

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

Tandatangan : …………………………….

Tarikh : …………………………….

Pengesahan Pegawai Keselamatan ICT

....
(Tandatangan & Cop Jawatan)

Tarikh: ....

* Polisi Keselamatan Siber boleh dicapai menerusi http://www.moa.gov.my

LAMPIRAN B

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 Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
11. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
12. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
13. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan 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.