KERAJAAN MALAYSIA

ARAHAN PENTADBIRAN KETUA PENGARAH MAMPU
BILANGAN 4 TAHUN 2020

POLISI KESELAMATAN SIBER MAMPU

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN
PENGURUSAN MALAYSIA (MAMPU)
JABATAN PERDANA MENTERI

KANDUNGAN

O

O

ARAHAN PENTADBIRAN KETUA PENGARAH MAMPU
BIL. 4 TAHUN 2020

POLISI KESELAMATAN SIBER MAMPU

TUJUAN

1. Pekeliling ini bertujuan untuk menjelaskan mengenai Polisi Keselamatan Siber (PKS), Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) yang perlu difahami dan dipatuhi oleh warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU.

LATAR BELAKANG

2. Berpandukan dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) yang berkuat kuasa pada 1 April 2016, MAMPU sentiasa memberi perhatian terhadap keselamatan siber yang merangkumi aset ICT di dalam dan di luar premis MAMPU bagi meminimumkan kesan gangguan ke atas sistem penyampaian perkhidmatan kerajaan.

3. PKS ini dibangunkan selaras dengan keperluan ISO/IEC 27001:2013 Information Security Management System (ISMS) yang merupakan amalan terbaik ISO/IEC 27000 dan *standard* antarabangsa dalam menetapkan keperluan secara berterusan sistem pengurusan keselamatan maklumat mengikut konteks organisasi.

BIDANG KAWALAN

4. Terdapat 14 bidang keselamatan yang merujuk kepada Annex A dalam piawaian ISO/IEC 27001:2013 Information Security Management Systems. 14 bidang tersebut adalah seperti di Jadual 1 di bawah:

Jadual 1: 14 Bidang Keselamatan

BIDANG	TAJUK
A.1	Polisi Keselamatan Maklumat
A.2	Perancangan Bagi Keselamatan Maklumat
A.3	Keselamatan Sumber Manusia
A.4	Pengurusan Aset
A.5	Kawalan Akses
A.6	Kriptografi
A.7	Keselamatan Fizikal Dan Persekitaran
A.8	Keselamatan Operasi
A.9	Pengurusan Komunikasi
A.10	Perolehan, Pembangunan Dan Penyelenggaraan Sistem
A.11	Hubungan Dengan Pembekal
A.12	Pengurusan Insiden Keselamatan Maklumat
A.13	Aspek Keselamatan Maklumat Dalam Pengurusan Kesinambungan Perkhidmatan
A.14	Pematuhan

Setiap bidang keselamatan ini diterangkan secara lebih terperinci di **Lampiran A.**

TANGGUNGJAWAB DAN PERANAN

5. Ahli-ahli Jawatankuasa ISMS, Pengurus ICT dan semua Pengarah Bahagian hendaklah bertanggungjawab sepenuhnya dalam melaksanakan kesemua bidang kawalan yang digariskan di dalam Polisi Keselamatan Siber MAMPU dan memastikan

polisi ini dipatuhi oleh semua warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU.

6. Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan dan dasar Kerajaan bagi memastikan dokumen sentiasa relevan.

7. Peranan dan tanggungjawab setiap individu yang terlibat dalam mencapai objektif Polisi Keselamatan Siber MAMPU diterangkan dengan lebih jelas dan teratur dalam Bidang kawalan A.6.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat seperti di **Lampiran A.**

IMPLIKASI KETIDAKPATUHAN

8. Ketidakpatuhan terhadap polisi keselamatan siber akan menjejaskan pengurusan ISMS MAMPU yang telah dipersijilkan ISMS sejak tahun 2010.

PEMAKAIAN

9. Polisi ini terpakai kepada semua warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU.

PEMBATALAN

10. Dengan berkuatkuasanya PKS ini, Dasar Keselamatan ICT (DKICT) versi 5.3 bertarikh 24 Mei 2010 adalah dibatalkan.

O

O

TARIKH BERKUAT KUASA

11. Polisi ini berkuat kuasa mulai tarikh dikeluarkan dan terpakai bagi tempoh lima tahun melainkan jika terdapat arahan terkini atau perkembangan baharu yang memerlukannya dikaji semula dan dikemas kini lebih awal sebelum tempoh tersebut berakhir.

PERTANYAAN

12. Sebarang pertanyaan mengenai polisi ini boleh dikemukakan kepada:

Pengarah,
Bahagian Pembangunan Perkhidmatan Gunasama Infrastruktur
dan Keselamatan ICT (BPG),
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU),
Jabatan Perdana Menteri,
Aras 1, Blok B, Bangunan MKN-Embassy Techzone,
No. 3200 Jalan Teknokrat 2,
63000 Cyberjaya, Selangor.

No. Telefon : 603-8872 5136
Emel : pks@mampu.gov.my

"BERKHIDMAT UNTUK NEGARA"

DATO' DR. YUSOF BIN ISMAIL
Ketua Pengarah MAMPU
24 September 2020
MAMPU.100 – 1/9/1 JLD 3 ( )

Diedarkan kepada:
Semua warga MAMPU

SENARAI RAJAH

TAKRIFAN

Bagi maksud pemakaian Arahan Pentadbiran Ketua Pengarah MAMPU Bil. 4 Tahun 2020 ini:

(1)	Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
(2)	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
(3)	Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
(4)	*Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
(5)	Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
(6)	*Bandwidth*	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
(7)	BCP/PKP	*Business Continuity Planning* Pelan Kesinambungan Perkhidmatan
(8)	CCTV	*Closed-Circuit Television System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam

SENARAI LAMPIRAN

Lampiran A

KERAJAAN MALAYSIA

POLISI KESELAMATAN SIBER MAMPU

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN
PENGURUSAN MALAYSIA (MAMPU)
JABATAN PERDANA MENTERI

KANDUNGAN

PERKARA **MUKA SURAT**

		premis pejabat bagi tujuan membantu pemantauan fizikal.
(9)	CIA	*Confidentiality, Integrity, Availability*
(10)	CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi.
(11)	*Clear Desk dan Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
(12)	*Data-at-rest* (data-dalam-simpanan)	*Refers to data that is being stored in stable destination systems. Data at rest is frequently defined as data that is not in use or is not traveling to system endpoints, such as mobile devices or workstations.*
(13)	*Data-in-motion* (data-dalam-pergerakan)	*Refers to a stream of data moving through any kind of network. It represents data which is being transferred or moved.*
(14)	*Data-in-use* (data-dalam-penggunaan)	*Refers to data that is not simply being passively stored in a stable destination, such as a central data warehouse, but is working its way through other parts of an IT architecture.*
(15)	*Denial of service*	Halangan pemberian perkhidmatan.
(16)	*Defence-in-depth*	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
(17)	*Downloading*	Aktiviti muat turun sesuatu perisian.

(18)	*Encryption*	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
(19)	*Escrow* (eskrow)	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
(20)	*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
(21)	*Forgery*	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).
(22)	CERT MAMPU	*Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT MAMPU.
(23)	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
(24)	*Hub*	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
(25)	ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi

(26)	ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
(27)	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
(28)	Impak fungsi jabatan	Melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.
(29)	Insiden Keselamatan	Musibah (adverse event) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
(30)	Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
(31)	*Internet Gateway*	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
(32)	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
(33)	ISDN	*Integrated Services Digital Network* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
(34)	*Intrusion Detection System (IDS)*	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya

		kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
(35)	*Intrusion Prevention System (IPS)*	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
(36)	ISMS	*Information Security Management System* Sistem Pengurusan Keselamatan Maklumat
(37)	MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
(38)	Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
(39)	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan
(40)	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
(41)	LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.

(42)	*Lock*	Mengunci komputer.
(43)	*Logout*	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
(44)	*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.
(45)	*Mobile Code*	*Mobile code* merupakan suatu perisian yang boleh dipindahkan di antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar internet.
(46)	MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
(47)	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
(48)	Pasukan ERT	Pasukan Tindakan Kecemasan/*Emergency Response Team* (ERT)
(49)	Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.

(50)	Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
(51)	Perisian Aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* atau pun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan
(52)	*Public-Key Infrastructure* (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perrkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
(53)	*Rollback* (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
(54)	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
(55)	Ruang siber	Sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT.
(56)	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
(57)	*Server*	Pelayan komputer

(58)	*Source Code*	Kod Sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia.
(59)	*Switches*	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense *Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu sistem penghantaran dengan mengurangkan perlanggaran yang berlaku.
(60)	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
(61)	*Uninterruptible Power Supply* (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
(62)	*Video Conference*	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa yang sama ia diterima oleh penghantar.
(63)	*Video Streaming*	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
(64)	Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
(65)	WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.

(66)	Warga MAMPU	Kakitangan kerajaan yang berkhidmat di MAMPU samada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT MAMPU
(67)	*Wireless LAN*	Jaringan komputer yang terhubung tanpa melalui kabel.
(68)	*Worm*	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

TUJUAN

1. Polisi Keselamatan Siber (PKS), Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU dalam melindungi maklumat di ruang siber.

LATAR BELAKANG

2. Polisi ini dibangunkan untuk menjamin kesinambungan urusan MAMPU dengan meminimumkan kesan insiden keselamatan siber. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi MAMPU bagi memastikan semua maklumat dilindungi.

OBJEKTIF

3. Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti yang berikut:

(i) Menerangkan kepada semua pengguna merangkumi warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber.

(ii) Memastikan keselamatan penyampaian perkhidmatan MAMPU di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

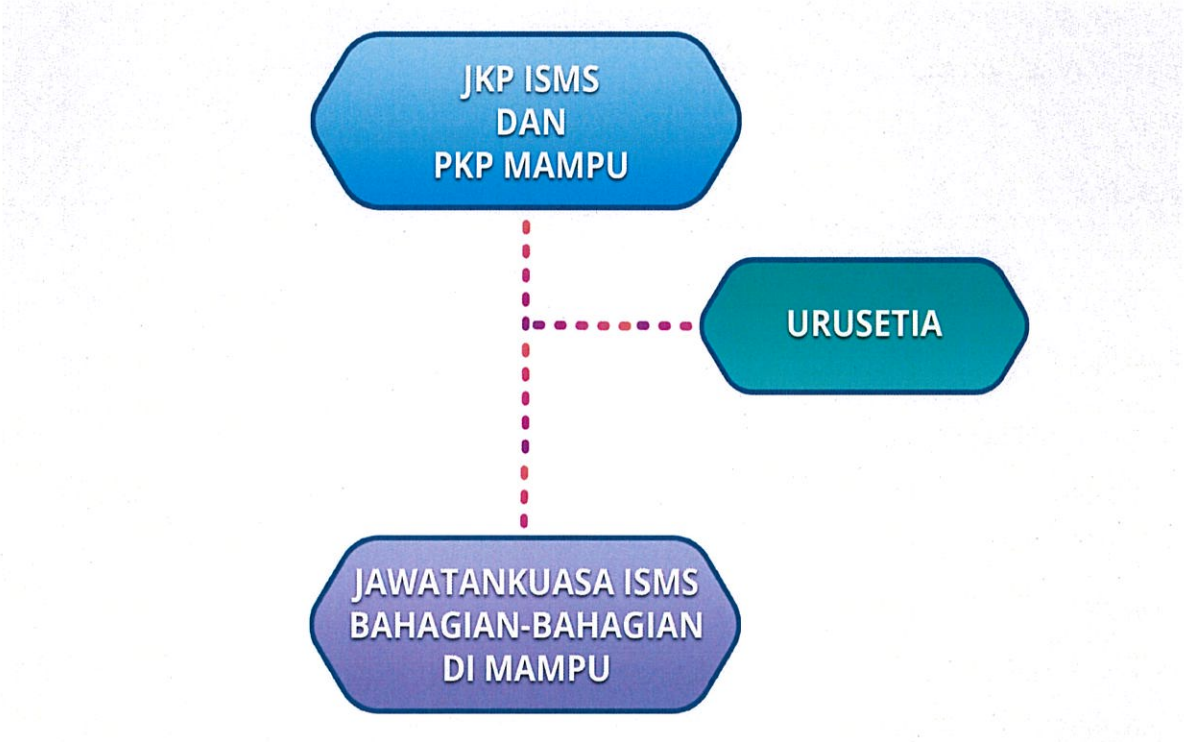
(iii) Memastikan kelancaran operasi MAMPU dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

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

(v) Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

TADBIR URUS

4. Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS MAMPU, satu (1) struktur tadbir urus iaitu Jawatankuasa Pemandu ISMS dan Pengurusan Kesinambungan Perkhidmatan MAMPU (JKPIM) telah diwujudkan seperti berikut:



Rajah 1: Struktur Jawatankuasa Pemandu ISMS dan PKP MAMPU

(i) Keahlian Jawatankuasa ini adalah seperti yang berikut

Pengerusi: Timbalan Ketua Pengarah (ICT)
MAMPU

Ahli:

i. Semua Ketua Perunding ICT;
ii. Semua Pengarah Bahagian;
iii. Pengarah MAMPU Sabah dan Sarawak; dan
iv. ICTSO MAMPU.

Urus Setia: Unit Pengurusan Keselamatan Maklumat,
Bahagian Perundingan ICT (BPI)

(ii) Bidang rujukan JKPIM adalah seperti yang berikut:

a) Menentukan halatuju keseluruhan pelaksanaan pensijilan ISMS MAMPU yang merangkumi perancangan, pemantauan dan pengesahan terhadap :

i. Pelaksanaan pensijilan ISMS ke atas perkhidmatan MAMPU yang dikenal pasti;

ii. Kelulusan ke atas dasar, objektif dan skop pelaksanaan ISMS;

iii. Penetapan kriteria penerimaan risiko, tahap risiko dan pelan penguraian risiko;

iv. Keputusan dan tindakan Mesyuarat Jawatankuasa ISMS Bahagian masing-masing;

v. Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan MAMPU yang dikenal pasti;

vi. Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik MAMPU;

vii. Keperluan ISMS diterapkan dalam budaya kerja pegawai MAMPU;

viii. Sumber yang diperlukan oleh pasukan pelaksana ISMS;

ix. Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya;

x. Pencapaian sasaran ISMS seperti yang dirancang;

xi. Arahan dan sokongan kepada Pasukan ISMS MAMPU bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan

xii. Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan.

ASET ICT MAMPU

5. Aset ICT MAMPU merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran seperti berikut:

(i) Maklumat

Semua penyedia perkhidmatan dalam MAMPU hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

(a) Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta

Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

(b) Maklumat Rasmi

Maklumat rasmi ialah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh MAMPU semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

(c) Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (PII atau Personally Identifiable Information) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

(d) Data Terbuka

Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. PII dikecualikan daripada data terbuka.

(ii) Aliran Data

Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi dalam MAMPU hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:

(a) Saluran komunikasi dan aliran data antara sistem di MAMPU;

(b) Saluran komunikasi dan aliran data ke sistem luar; dan

(c) Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

(iii) Platform Aplikasi dan Perisian

Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

(iv) Peranti Fizikal dan Sistem

Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

(a) Pelayan;

(b) Peranti/Peralatan Rangkaian;

(c) Komputer Peribadi/Komputer Riba;

(d) Telefon/peranti pintar;

(e) Media Storan;

(f) Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);

(g) Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan; dan

(h) Peranti pengesahan (authentication devices), contohnya token keselamatan, *dongle* dan alat pengimbas biometrik.

(v) Sistem Luaran

Sistem luaran ialah sistem bukan milik MAMPU yang dihubungkan dengan sistem MAMPU. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

(vi) Sumber Luaran

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi MAMPU. Contoh perkhidmatan sumber luaran ialah:

(a) Perisian Sebagai Satu Perkhidmatan

(b) Platform Sebagai Satu Perkhidmatan

(c) Infrastruktur Sebagai Satu Perkhidmatan

(d) Storan Pengkomputeran Awan

(e) Pemantauan Keselamatan

Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala.

RISIKO

6. MAMPU hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian MAMPU tidak dapat melaksanakan fungsi jabatan dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber MAMPU.

7. Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber MAMPU.

8. Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

(i) Kerentanan

Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

(ii) Ancaman

MAMPU hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

(iii) Impak

MAMPU hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi MAMPU.

(iv) Tahap Risiko

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

(v) Penguraian Risiko

(a) Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

(b) Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

(1) Teknologi

Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, tembok api digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

(2) Proses

Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

(3) Manusia

Mengenal pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

(vi) Pengurusan Risiko

(a) Penyedia perkhidmatan digital di MAMPU hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

(1) mengenal pasti kerentanan;

(2) mengenal pasti ancaman;

(3) menilai risiko;

(4) menentukan penguraian risiko;

(5) memantau keberkesanan penguraian risiko; dan

(6) memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

(b) Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **sekali setahun** oleh Bahagian masing-masing dan dimaklumkan kepada Mesyuarat Jawatankuasa Pemandu ISMS dan PKP MAMPU.

PRINSIP KESELAMATAN

9. Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, MAMPU hendaklah melaksanakan prinsip keselamatan seperti yang berikut:

(i) Prinsip "Perlu-Tahu"

MAMPU hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip "Perlu-Tahu" yang membenarkan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja.

Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi, peranan dan fungsi pengguna tersebut.

(ii) Hak Keistimewaan Minimum

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses 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. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

(iii) Pengasingan Tugas

Bagi mengekalkan prinsip sekat-dan-imbang (check and balance), MAMPU hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

(iv) Kawalan Capaian Berdasarkan Peranan

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

(v) Peminimuman Data

MAMPU hendaklah mengamalkan prinsip peminimuman data yang mengehadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

TEKNOLOGI

10. Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data di setiap elemen pengkomputeran seperti berikut:

(i) Peringkat Pemprosesan Data

(a) Data-dalam-simpanan

(1) MAMPU hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.

(2) Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

(b) Data-dalam-pergerakan

MAMPU hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan

langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-pergerakan.

(c) Data-dalam-penggunaan

(1) MAMPU hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

(2) Teknologi yang bersesuaian boleh digunakan oleh MAMPU untuk memastikan asal data dan data/transaksi tanpa-sangkal.

(d) Perlindungan Ketirisan Data

(1) Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

(2) Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

(ii) Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, MAMPU hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (countermeasure dan control measure) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan yang dikeluarkan oleh Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan dari CGSO.

Setiap projek ICT yang dibangunkan di MAMPU hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

(a) Peranti pengkomputeran peribadi

(1) Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet, dan peranti storan.

(2) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada MAMPU. Walau bagaimanapun, peranti pengkomputeran peribadi milik pensendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

(b) Peranti rangkaian

(1) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti VPN dan kabel.

(2) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(c) Aplikasi

(1) Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.

(2) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(d) Pelayan

(1) Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

(2) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(e) Persekitaran fizikal

(1) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

(2) MAMPU hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

(3) Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.

(4) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

PROSES

11. Warga MAMPU hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

(i) Konfigurasi Asas

(a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.

(b) Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

(ii) Kawalan Perubahan Konfigurasi

(a) Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

(b) Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.

(c) Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

(iii) Sandaran

(a) Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.

(b) Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

(iv) Kitaran Pengurusan Aset

(a) Pindah

(1) Pemindahan hak milik aset berlaku dalam keadaan berikut:

(i) Warga MAMPU meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;

(ii) Aset yang dikongsi untuk kegunaan sementara;

(iii) Pemberian aset kepada agensi lain; dan

(iv) Aset dikembalikan setelah tamat tempoh sewaan.

(2) Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (b).

(b) Pelupusan

(1) Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.

(2) Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.

(3) Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.

(4) Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

(c) Kitaran Hayat

(1) Kitaran hayat data hendaklah diuruskan mengikut Akta 629.

(2) Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

MANUSIA

12. Warga MAMPU, pembekal, pakar runding dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

13. Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan pengguna hendaklah dibangunkan bagi semua warga MAMPU.

(i) Kompetensi Pengguna

(a) Kompetensi pengguna termasuk:

(1) Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber.

(2) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga MAMPU berhubung alat-alat

keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

(b) Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

(c) Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

(ii) Kompetensi Pelaksana

(a) Warga MAMPU yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

(b) Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

(1) Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.

(2) Memenuhi keperluan pembelajaran berterusan.

(3) Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.

(4) Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

(c) Pegawai Keselamatan ICT yang dilantik oleh MAMPU hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di MAMPU.

(iii) Peranan

(a) Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

(b) Setiap orang yang 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.

(c) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.

(d) Warga MAMPU yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.

(e) Warga MAMPU yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.

(f) Warga MAMPU lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan.

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

14. Setiap projek di MAMPU hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.

15. Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), Polisi Keselamatan Siber MAMPU dan surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.

16. Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.

17. Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

(i) Peranti Pengkomputeran Peribadi

(a) Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet dan peranti storan.

(b) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada MAMPU. Walau bagaimanapun, peranti pengkomputeran peribadi milik pensendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

(ii) Peranti Rangkaian

(a) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti VPN dan kabel.

(b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(iii) Aplikasi

(a) Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.

(b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(iv) Pelayan

(a) Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

(b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(v) Persekitaran Fizikal

(a) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

(b) MAMPU hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

(c) Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.

(d) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

PERNYATAAN POLISI KESELAMATAN SIBER MAMPU

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

19. Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(i) Kerahsiaan

Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

(ii) Integriti

Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan.

(iii) Tidak Boleh Disangkal

Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

(iv) Kesahihan

Data dan maklumat hendaklah dipastikan kesahihannya.

(v) Ketersediaan

Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

20. Selain itu, langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT MAMPU, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

21. 14 bidang keselamatan yang terlibat di dalam Polisi Keselamatan Siber MAMPU diterangkan dengan lebih jelas dan teratur seperti berikut:

BIDANG A.1 : POLISI KESELAMATAN MAKLUMAT (INFORMATION SECURITY POLICY)

A.1.1 Hala Tuju Pengurusan Untuk Keselamatan Maklumat (Management Directions for Information Security)

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

A.1.1.1 Polisi Keselamatan Maklumat (Policies for Information Security)

Peranan: JPICT/CIO/ ICTSO/ Pengarah Bahagian

Pelaksanaan polisi ini akan dijalankan oleh Ketua Pengarah MAMPU dengan disokong oleh Jawatankuasa Pemandu ICT, JKP ISMS & PKP yang terdiri daripada Ketua Pegawai Maklumat, Pegawai Keselamatan ICT, Pengarah-pengarah Bahagian, Pengarah MAMPU Cawangan Sabah dan Sarawak dan ahli-ahli yang dilantik oleh Ketua Pengarah MAMPU.

Polisi Keselamatan Siber MAMPU mestilah dipatuhi oleh semua warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU.

Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan MAMPU kepada warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU.

A.1.1.2 Kajian Semula Polisi untuk Keselamatan Maklumat (Review of Policies for Information Security)

Peranan: JPICT/CIO/ICTSO

Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan. Berikut ialah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber MAMPU:

(i) Mengenal pasti dan menentukan perubahan yang diperlukan;

(ii) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan;

(iii) Memaklumkan pindaan yang telah disahkan oleh JPICT kepada warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU; dan

(iv) Polisi ini hendaklah dikaji semula setiap **LIMA (5) TAHUN SEKALI** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.

BIDANG A.2 : PERANCANGAN BAGI KESELAMATAN ORGANISASI (ORGANIZATION OF INFORMATION SECURITY)

A.2.1 Perancangan Dalaman (Internal Organization)

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

A.2.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat (The Role and Responsibility of Information Security)

(i) Ketua Pengarah

Peranan: Ketua Pengarah

Peranan dan tanggungjawab adalah seperti yang berikut:

(a) Memastikan penguatkuasaan pelaksanaan Polisi ini;

(b) Memastikan warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini;

(c) Memastikan semua keperluan MAMPU seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi;

(d) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan

(e) Melantik CIO dan ICTSO.

(ii) Ketua Pegawai Maklumat (CIO)

Peranan: CIO MAMPU

Peranan dan tanggungjawab CIO adalah seperti yang berikut:

(a) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam Polisi ini;

(b) Memastikan kawalan keselamatan maklumat dalam MAMPU diseragam dan diselaraskan dengan sebaiknya;

(c) Memastikan Pelan Strategik ICT MAMPU mengandungi aspek keselamatan siber; dan

(d) Menyelaras pelan latihan dan program kesedaran keselamatan siber.

(iii) Pegawai Keselamatan ICT (ICTSO)

Peranan: ICTSO

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti yang berikut:

(a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini;

(b) Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa;

(c) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

(d) Melaporkan insiden keselamatan siber kepada CERT MAMPU dan seterusnya membantu dalam penyiasatan atau pemulihan;

(e) Melaporkan insiden keselamatan siber kepada CIO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP);

(f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera;

(g) Melaksanakan pematuhan Polisi ini oleh warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU;

(h) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; dan

(i) Menyedia dan merangka latihan dan program kesedaran keselamatan siber.

(iv) Pengarah Bahagian

Peranan: Pengarah Bahagian

Peranan dan tanggungjawab Pengarah Bahagian ialah melaksanakan keperluan Polisi ini dalam operasi semasa seperti yang berikut:

(a) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru;

(b) Pembelian atau peningkatan perisian dan sistem komputer;

(c) Perolehan teknologi dan perkhidmatan komunikasi baru;

(d) Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan

(e) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa.

(v) Pentadbir Sistem ICT

Peranan: Pentadbir Sistem ICT

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti yang berikut:

(a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;

(b) Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini;

(c) Memantau aktiviti capaian sistem aplikasi;

(d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta;

(e) Menganalisis dan menyimpan rekod jejak audit;

(f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan

(g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel di dalam keadaan yang baik.

(vi) Jawatankuasa Pemandu ICT (JPICT)

Peranan: Pentadbir Sistem ICT

Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil 3 Tahun 2015 ialah merancang dan menentukan langkah-langkah keselamatan siber.

(vii) Jawatankuasa Pemandu ISMS dan PKP

Peranan: Jawatankuasa Pemandu ISMS dan PKP

Bidang rujukan Jawatankuasa Pemandu ISMS dan PKP adalah seperti yang berikut:

(a) Menentukan hala tuju keseluruhan pelaksanaan pensijilan ISMS MAMPU yang merangkumi perancangan, pemantauan dan pengesahan terhadap:

(b) Pelaksanaan pensijilan ISMS ke atas perkhidmatan MAMPU yang dikenal pasti;

(c) Kelulusan ke atas dasar, objektif dan skop pelaksanaan ISMS;

(d) Penetapan kriteria penerimaan risiko, tahap risiko dan risk treatment plan;

(e) Keputusan dan tindakan Mesyuarat Jawatankuasa ISMS Bahagian masing-masing;

(f) Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan MAMPU yang dikenal pasti;

(g) Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik MAMPU;

(h) Keperluan ISMS diterapkan dalam budaya kerja pegawai MAMPU;

(i) Sumber yang diperlukan oleh pasukan pelaksana ISMS;

(j) Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya;

(k) Pencapaian sasaran ISMS seperti yang dirancang;

(l) Arahan dan sokongan kepada Pasukan ISMS MAMPU bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan

(m) Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan.

Meluluskan:

(a) Struktur organisasi ISMS dan PKP MAMPU;

(b) Keperluan sumber; dan

(c) Pelantikan Pasukan Audit dalam ISMS MAMPU.

(viii) Computer Emergency Response Team (CERT) MAMPU

Peranan: CERT MAMPU

Peranan dan tanggungjawab CERT MAMPU adalah seperti yang berikut:

(a) Menerima dan mengesan aduan keselamatan siber serta menilai tahap dan jenis insiden;

(b) Merekod dan menjalankan siasatan awal insiden yang diterima;

(c) Menangani tindak balas insiden keselamatan siber dan mengambil tindakan baik pulih minimum;

(d) Menasihati Pentadbir Sistem/Pelayan untuk mengambil tindakan pemulihan dan pengukuhan; dan

(e) Menyebarkan makluman berkaitan pengukuhan keselamatan siber kepada Pentadbir Sistem ICT.

(ix) Pengguna

Peranan: Pengguna

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

(a) Membaca, memahami dan mematuhi Polisi ini;

(b) Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya;

(c) Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat;

(d) Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan;

(e) Melaksanakan langkah-langkah perlindungan seperti yang berikut:

(1) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(2) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;

(3) Menentukan maklumat sedia untuk digunakan;

(4) Menjaga kerahsiaan maklumat;

(5) Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan;

(6) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

(7) Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum.

(f) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CERT MAMPU dengan segera;

(g) Menghadiri program-program kesedaran mengenai keselamatan siber; dan

(h) Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini.

A.2.1.2 Pengasingan Tugas (Segregation of Duties)

Peranan: Pengarah Bahagian

Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;

(ii) tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi;

(iii) perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan

(iv) pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

A.2.1.3 Hubungan Dengan Pihak Berkuasa (Contact with Authorities)

Peranan: Bahagian Khidmat Pengurusan (BKP) MAMPU, Pasukan ERT, CERT MAMPU

Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab MAMPU;

(ii) mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan

(iii) insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.

A.2.1.4 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus (Contact with Special Interest Groups)

Peranan: Warga MAMPU (Mengikut Bidang Kepakaran)

Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau pun forum bagi:

(i) meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;

(ii) menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini;

(iii) berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan

(iv) berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

A.2.1.5 Keselamatan Maklumat dalam Pengurusan Projek (Information Security in Project Management)

Peranan: Warga MAMPU (Pasukan Projek)

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(a) keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek MAMPU;

(b) objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;

(c) pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;

(d) kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber MAMPU; dan

(e) penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.

A.2.2 Peranti mudah alih dan telekerja (Mobile Devices and Teleworking)

Objektif: Memastikan keselamatan telekerja dan penggunaan peralatan mudah alih.

A.6.2.1 Polisi Peranti Mudah Alih (Mobile Device Policy)

(i) Peranan: Sokongan Teknikal MAMPU (STM)

Membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih.

(ii) Peranan: JPICT

Meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga MAMPU.

(iii) Peranan: Warga MAMPU

Perkara-perkara yang perlu dipatuhi:

(a) pendaftaran ke atas peralatan mudah alih;

(b) keperluan ke atas perlindungan secara fizikal;

(c) kawalan ke atas pemasangan perisian peralatan mudah alih;

(d) kawalan ke atas versi dan *patches* perisian;

(e) sekatan ke atas akses perkhidmatan maklumat secara dalam talian;

(f) kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan

(g) peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.

A.2.2.2 Telekerja (Teleworking)

Peranan: Warga MAMPU

Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja.

BIDANG A.3: KESELAMATAN SUMBER MANUSIA (HUMAN RESOURCE SECURITY)

A.3.1 Sebelum Perkhidmatan (Prior To Employment)

Objektif: Memastikan warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

A.3.1.1 Tapisan Keselamatan (Security Screening)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Tapisan keselamatan hendaklah dijalankan terhadap warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan

(ii) menjalankan tapisan keselamatan untuk warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

A.3.1.2 Terma dan Syarat Perkhidmatan (Terms and Conditions of Employment)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Persetujuan berkontrak dengan warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

(i) menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU yang terlibat dalam menjamin keselamatan aset ICT; dan

(ii) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

A.3.2 Dalam Tempoh Perkhidmatan (During Deployment)

Objektif: Memastikan warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

A.3.2.1 Tanggungjawab Pengurusan (Management Responsibilities)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Pengurusan hendaklah memastikan warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.

A.3.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat (Information Security Awareness, Education and Training)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber MAMPU, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;

(ii) memastikan kesedaran yang berkaitan Polisi Keselamatan Siber MAMPU perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan

(iii) memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

A.3.2.3 Proses Tatatertib (Disciplinary Process)

Pengguna: BKP

Proses tatatertib yang formal dan disampaikan kepada warga MAMPU hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga MAMPU yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga MAMPU sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh MAMPU;

(ii) Warga MAMPU yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT MAMPU.

A.3.3 Penamatan dan Pertukaran Perkhidmatan (Termination and Change of Employment)

Objektif: Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas warga MAMPU diurus dengan teratur.

A.3.3.1 Penamatan atau Pertukaran Tanggung Jawab Perkhidmatan (Termination or Change of Employment Responsibilities)

Peranan: STM dan warga MAMPU

Warga MAMPU yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut:

(i) Memastikan semua aset ICT dikembalikan kepada MAMPU mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

(ii) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan MAMPU dan/atau terma perkhidmatan yang ditetapkan.

(iii) Maklumat rasmi MAMPU dalam peranti tidak dibenarkan dibawa keluar dari MAMPU.

Warga MAMPU yang telah bertukar perkhidmatan hendaklah:

(i) memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada MAMPU mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

(ii) menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.

BIDANG A.4 : PENGURUSAN ASET (ASET MANAGEMENT)

A.4.1 Tanggungjawab Terhadap Aset (Responsibility for Assets)

Objektif: Untuk mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MAMPU.

A.4.1.1 Inventori Aset (Inventory of Assets)

Peranan: Pegawai Penerima Aset, Pegawai Aset dan warga MAMPU

Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT MAMPU. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:

(i) MAMPU hendaklah mengenal pasti Pegawai Penerima Aset setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT

(ii) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa.

(iii) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;

(iv) Pegawai Aset hendaklah mengesahkan penempatan aset ICT.

A.4.1.2 Pemilikan Aset (Ownership of Assets)

Peranan: Pegawai Aset dan warga MAMPU

Aset yang diselanggara hendaklah hak milik MAMPU. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut:

(i) memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset;

(ii) memastikan aset telah dikelaskan dan dilindungi;

(iii) kenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;

(iv) memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan

(v) memastikan semua jenis aset dipelihara dengan baik.

A.4.1.3 Penggunaan Aset yang Dibenarkan (Acceptable Use of Assets)

Peranan: Warga MAMPU

Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.

A.4.1.4 Pemulangan Aset (Return of Assets)

Peranan: Warga MAMPU

Warga MAMPU hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.

A.4.2 Pengelasan Maklumat (Information Classification)

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

A.4.2.1 Pengelasan Maklumat (Classification of Information)

Peranan: Pegawai Pengelasan

Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.

A.4.2.2 Pelabelan Maklumat (Labelling of Information)

Peranan: Warga MAMPU

Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.

A.4.2.3 Pengendalian Aset (Handling of Assets)

Peranan: Warga MAMPU

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

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa;

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

vi. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

vii. Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

A.4.3 Pengendalian Media (Media Handling)

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

A.4.3.1 Pengurusan Media Boleh Alih (Management of Removal Media)

Peranan: Pentadbir Sistem ICT dan Pengguna

Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh MAMPU. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:

(i) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;

(ii) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;

(iii) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;

(iv) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan

(v) Menyimpan semua jenis media di tempat yang selamat.

A.4.3.2 Pelupusan Media (Disposal of Media)

Peranan: Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.

(i) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan.

(ii) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.

A.4.3.3 Pemindahan Media Fizikal (Physical Media Transfer)

Peranan: Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.

(i) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan.

(ii) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.

BIDANG A.5 : KAWALAN AKSES (ACCESS CONTROL)

A.5.1 Kawalan Akses (Business Requirements of Access Control)

Objektif: Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.

A.5.1.1 Polisi Kawalan Akses (Access Control Policy)

Peranan: Pemilik perkhidmatan digital dan Pentadbir Sistem ICT.

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza.

Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Keperluan keselamatan aplikasi;

(ii) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian;

(iii) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa;

(iv) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;

(v) Pengasingan peranan kawalan capaian;

(vi) Kebenaran rasmi permintaan akses;

(vii) Keperluan semakan hak akses berkala;

(viii) Pembatalan hak akses;

(ix) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan

(x) Capaian *privilege*.

A.5.1.2 Capaian kepada Rangkaian dan Perkhidmatan Rangkaian (Access to Networks and Network Services)

Peranan: ICTSO, Pengarah Bahagian dan Pentadbir Rangkaian

Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari MAMPU. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

(i) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian MAMPU, rangkaian agensi lain dan rangkaian awam;

(ii) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan

(iii) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

A.5.2 Pengurusan Akses Pengguna (User Access Management)

Objektif: Akses 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.

A.5.2.1 Pendaftaran dan Pembatalan Pengguna (User Registration and De-Registration)

Peranan: Semua Pengguna dan warga MAMPU

Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara–perkara berikut hendaklah dipatuhi:

(i) Akaun yang diperuntukkan oleh MAMPU sahaja boleh digunakan;

(ii) Akaun pengguna mestilah unik;

(iii) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada MAMPU terlebih dahulu;

(iv) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan

(v) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan MAMPU.

A.5.2.2 Peruntukan Akses Pengguna (User Access Provisioning)

Peranan: Pentadbir Sistem ICT dan Pengarah Bahagian

Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.

A.5.2.3 Pengurusan Hak Akses Istimewa (Management of Privileged Access Rights)

Peranan: Pentadbir Sistem ICT

Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal.

Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada **Prosedur Pendaftaran dan Penamatan Pengguna.**

A.5.2.4 Pengurusan Maklumat Pengesahan Rahsia Pengguna (Management of Secret Authentication Information of Users)

Peranan: ICTSO dan Pentadbir Sistem ICT

Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.

A.5.2.5 Kajian Semula Hak Akses Pengguna (Review of User Access Rights)

Peranan: ICTSO dan Pentadbir Sistem ICT

Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan.
Pentadbir Sistem ICT perlu mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.

A.5.2.6 Pembatalan atau Pelarasan Hak Akses (Removal or Adjustment of Access Rights)

Peranan: Pentadbir Sistem ICT dan Pengarah Bahagian

Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam MAMPU.

A.5.3 Tanggungjawab Pengguna (User Responsibilities)

Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.

A.5.3.1 Penggunaan Maklumat Pengesahan Rahsia (Use of Secret Authentication Information)

Peranan: Pengguna, Pentadbir Sistem ICT dan Pengarah Bahagian

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

(i) Membaca, memahami dan mematuhi Polisi Keselamatan Siber MAMPU;

(ii) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;

(iii) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat MAMPU;

(iv) Melaksanakan langkah-langkah perlindungan seperti yang berikut:

(a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;

(c) Menentukan maklumat sedia untuk digunakan;

(d) Menjaga kerahsiaan kata laluan;

(e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

(f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

(g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

(v) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan

(vi) Menghadiri program-program kesedaran mengenai keselamatan siber.

A.5.3.2 Penggunaan Maklumat Pengesahan Rahsia (Use of Secret Authentication Information)

Peranan: Pengguna, Pentadbir Sistem, ICTSO, Pengarah Bahagian

Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.

A.5.4 Kawalan Akses Sistem dan Aplikasi (System and Application Access Control)

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

A.5.4.1 Sekatan Akses Maklumat (Information Access Restriction)

Peranan: Pengguna, Pentadbir Sistem, ICTSO, Pengarah Bahagian

Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.

A.5.4.2 Prosedur Log Masuk yang Selamat (Secure Log-On Procedure)

Peranan: Pentadbir Sistem, ICTSO, Pengarah Bahagian

Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak

dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut:

(i) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan MAMPU;

(ii) Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem;

(iii) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin;

(iv) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna;

(v) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti;

(vi) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.

A.5.4.3 Sistem Pengurusan Kata Laluan (Password Management System)

Peranan: Pengguna, Pentadbir Sistem, ICTSO, Pengarah Bahagian

Sistem pengurusan kata laluan hendaklah interaktif dan mengambilkira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MAMPU seperti yang berikut:

(i) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

(ii) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

(iii) Panjang kata laluan mestilah sekurang kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) **KECUALI** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad.

(iv) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun;

(v) Kata laluan paparan kunci (lock screen) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

(vi) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara;

(vii) Kuat kuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan;

(viii) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

(ix) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan

(x) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.

A.5.4.4 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa (Use of Privileged Utility Programs)

Peranan: Pentadbir Sistem ICT, Pengarah Bahagian

Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.

A.5.4.5 Kawalan Akses Kepada Kod Sumber Program (Access Control to Program Source Code)

Peranan: Pengarah Projek, Pengurus Projek dan Pentadbir Sistem ICT

Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Log audit perlu dikekalkan kepada semua akses kepada kod sumber;

(ii) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan

(iii) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik MAMPU.

BIDANG A.6 : KRIPTOGRAFI (CRYPTOGRAPHY)

A.6.1 Kawalan Kriptografi (Cryptography Controls)

Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan, dan/atau keutuhan maklumat.

A.6.1.1 Polisi Pengunaan Kawalan Kriptografi (Policy on The Use of Cryptographic Control)

Peranan: Pengarah Projek

Kriptografi merangkumi kaedah-kaedah seperti yang berikut:

(i) Enkripsi

Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (encryption).

(ii) Tandatangan Digital

Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan.

A.6.1.2 Pengurusan Kunci Awam (Public Key Management)

Peranan: Warga MAMPU dan Pengarah Bahagian Pembangunan Perkhidmatan Gunasama Infrastruktur dan Keselamatan ICT (BPG)

Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam/*Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

BIDANG A.7 : KESELAMATAN FIZIKAL DAN PERSEKITARAN (PHYSICAL AND ENVIRONMENTAL SECURITY)

A.7.1 Kawasan Selamat (Secure Areas)

Objektif: Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat MAMPU.

A.7.1.1 Perimeter Keselamatan Fizikal (Physical Security Parameter)

Peranan: Pejabat Ketua Pegawai Keselamatan Kerajaan, BKP

Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan Aset ICT MAMPU. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

(i) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;

(ii) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;

(iii) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;

(iv) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia;

(v) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad;

(vi) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan

(vii) Memasang alat penggera atau kamera keselamatan;

A.7.1.2 Kawalan Kemasukan Fizikal (Physical Entry Controls)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis MAMPU. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Setiap pegawai dan kakitangan MAMPU hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada MAMPU apabila bertukar, tamat perkhidmatan atau bersara;

(ii) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; dan

(iii) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan Aset ICT MAMPU; dan

(iv) Kehilangan pas hendaklah dilaporkan segera kepada Pihak Berkuasa.

A.7.1.3 Keselamatan Pejabat, Bilik dan Kemudahan (Securing Offices, Rooms and Facilities)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran;

(ii) Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan

(iii) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.

A.7.1.4 Perlindungan Daripada Ancaman Luar Dan Persekitaran (Protecting Against External and Environmental Threats)

Peranan: Pentadbir Pusat Data dan BKP

Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. MAMPU perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.

A.7.1.5 Bekerja di Kawasan Selamat (Working in Secure Area)

Peranan: Pentadbir Pusat Data dan BKP

Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga MAMPU yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis MAMPU termasuklah Pusat Data.

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut:

(i) Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik *server* atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran;

(ii) Akses adalah terhad kepada warga MAMPU yang telah diberi kuasa sahaja dan dipantau pada setiap masa;

(iii) Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai;

(iv) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;

(v) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;

(vi) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;

(vii) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam;

(viii) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan;

(ix) Memperkukuh dinding dan siling; dan

(x) Mengehadkan jalan keluar masuk.

A.7.1.6 Kawasan Penyerahan dan Pemunggahan (Delivery and Loading Areas)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Titik kemasukan *access point* seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan.

MAMPU hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.

A.7.2 Peralatan ICT (ICT Equipment)

Objektif: Melindungi peralatan ICT MAMPU daripada kehilangan, kerosakan, kecurian dan disalahgunakan.

A.7.2.1 Penempatan dan Perlindungan Peralatan ICT (Equipment Sitting and Protection)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:

(i) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

(ii) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

(iii) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

(iv) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;

(v) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

(vi) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna;

(vii) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;

(viii) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set);

(ix) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan.

(x) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci;

(xi) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai;

(xii) Peralatan ICT yang hendak dibawa ke luar premis MAMPU, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;

(xiii) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;

(xiv) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

(xv) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

(xvi) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih;

(xvii) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

(xviii) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;

(xix) Pengguna dilarang sama sekali mengubah ***password administrator*** yang telah ditetapkan oleh pihak ICT; dan

(xx) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan MAMPU sahaja.

A.7.2.2 Utiliti Sokongan (Supporting Utilities)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).

A.7.2.3 Keselamatan Kabel (Cabling Security)

Peranan: Pentadbir Sistem ICT

Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan.

(i) Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:

(ii) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;

(iii) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;

(iv) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

(v) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.

A.7.2.4 Penyelenggaraan Peralatan (Equipment Maintenance)

Peranan: Pegawai Aset, Pentadbir Sistem ICT

Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

(i) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;

(ii) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;

(iii) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

(iv) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan

(v) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

A.7.2.5 Pengalihan Aset (Removal of Assets)

Peranan: Pengguna, Pegawai Aset

Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

(i) Peralatan ICT yang hendak dibawa keluar dari premis MAMPU untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Pengarah MAMPU atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan

(ii) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.

A.7.2.6 Keselamatan Peralatan dan Aset di Luar Premis (Security of Equipment Off-Premises)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis MAMPU. Peralatan yang dibawa keluar dari premis MAMPU adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Peralatan perlu dilindungi dan dikawal sepanjang masa;

(ii) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan

(iii) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.

A.7.2.7 Pelupusan yang Selamat atau Penggunaan Semula Peralatan (Secure Disposal or Re-Use of Equipment)

Peranan: Pegawai Aset, Pentadbir Sistem ICT dan warga MAMPU

Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (overwrite) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MAMPU dan ditempatkan di MAMPU.

Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan MAMPU. Langkah-langkah seperti yang berikut hendaklah diambil:

(i) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat;

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

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

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

(v) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti yang berikut:

(a) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.

(b) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *CPU* seperti *RAM*, *Hardisk*, *Motherboard* dan sebagainya.

(c) Menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR*, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MAMPU.

(d) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan

(e) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MAMPU.

(vi) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumbdrive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

(vii) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan;

(viii) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa;

(ix) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan

(x) Pegawai~~–asset~~ aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori MyAsset.

A.7.2.8 Peralatan Pengguna Tanpa Kawalan (Unattended User Equipment)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:

(i) Tamatkan sesi aktif apabila selesai tugas;

(ii) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan

(iii) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.

A.7.2.9 Dasar Meja Kosong dan Skrin Kosong (Policy Clear Desk dan Clear Screen)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Clear Desk bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuklah seperti yang berikut:

(i) Menggunakan kemudahan *password screensaver* atau *logout* apabila meninggalkan komputer;

(ii) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;

(iii) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.

(iv) E-mel masuk dan keluar hendaklah dikawal; dan

(v) Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.

BIDANG A.8 : KESELAMATAN OPERASI (OPERATIONS SECURITY)

A.8.1 Prosedur dan Tanggungjawab Operasi (Operational Procedures and Responsibilities)

Objektif: Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat.

A.8.1.1 Prosedur Operasi yang Didokumenkan (Documented Operating Procedures)

Peranan: Pengarah Bahagian dan Pentadbir Sistem ICT

Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut:

(i) semua prosedur keselamatan siber yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;

(ii) setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan

(iii) semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.

A.8.1.2 Pengurusan Perubahan (Change Management)

Peranan: Pentadbir Sistem ICT

Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia

dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut:

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

(ii) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;

(iii) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan

(iv) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.

A.8.1.3 Pengurusan Kapasiti (Capacity Management)

Peranan: Pemilik Sistem, Pentadbir Sistem

Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) 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; dan

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

A.8.1.4 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi (Separation of Development, Test and Operational Facilities)

Peranan: Pentadbir Sistem ICT

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (production).

(ii) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan

(iii) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

A.8.2 Perlindungan Daripada Perisian Hasad (Protection from Malware)

Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.

A.8.2.1 Kawalan Daripada Perisian Hasad (Controls Against Malware)

Peranan: Pentadbir Sistem ICT, Pengguna

Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut.

Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut:

(a) Memasang sistem keselamatan untuk mengesan perisian atau program *malware* seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;

(b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;

(c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;

(d) Mengemas kini antivirus dengan *signature/pattern* antivirus yang terkini;

(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

(f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

(g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; dan

(h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.

A.8.3 Sandaran (Backup)

Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.

A.8.3.1 Sandaran Maklumat (Information Backup)

Peranan: Pentadbir Sistem ICT

Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off site*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;

(ii) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi;

(iii) Menguji sistem sandaran sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan

(iv) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara **harian, mingguan, bulanan atau tahunan**. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya **TIGA (3) GENERASI.**

A.8.4 Pengelogan dan Pemantauan (Logging and Monitoring)

Objektif: Merekodkan peristiwa dan menghasilkan bukti.

A.8.4.1 Pengelogan Kejadian (Event Logging)

Peranan: Pentadbir Sistem ICT

Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.

Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut:

(i) Fail log sistem pengoperasian;

(ii) Fail log servis (contoh: *web*, e-mel);

(iii) Fail log aplikasi (audit trail); dan

(iv) Fail log rangkaian (contoh: *switch, firewall, IPS*).

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

(i) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

(ii) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan

(iii) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada pasukan CERT MAMPU.

A.8.4.2 Perlindungan Maklumat Log (Protection of Log Information)

Peranan: Pentadbir Sistem ICT

Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.

A.8.4.3 Log pentadbir dan Pengendali (Administrator and Operator Logs)

Peranan: Pentadbir Sistem ICT dan CERT MAMPU

Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap.

(i) Memantau penggunaan kemudahan memproses maklumat secara berkala;

(ii) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu;

(iii) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;

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

(v) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada pasukan CERT MAMPU.

A.8.4.4 Penyeragaman Jam (Clock Synchronisation)

Peranan: Pentadbir Pusat Data

Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MAMPU atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh National Metrology Institute of Malaysia (NMIM).

A.8.5 Kawalan Perisian yang Beroperasi (Control of Operational Software)

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

A.8.5.1 Pemasangan Perisian Pada Sistem yang Beroperasi (Installation of Software on Operational Systems)

Peranan: Pengarah Bahagian dan Pentadbir Sistem ICT

Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut:

(i) Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;

(ii) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan

(iii) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

A.8.6 Pengurusan Kerentanan Teknikal (Technical Vulnerability Management)

Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.

A.8.6.1 Pengurusan Kerentanan Teknikal (Management of Technical Vulnerabilities)

Peranan: Pentadbir Sistem ICT dan CERT MAMPU

Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;

(ii) Menganalisis tahap risiko kerentanan; dan

(iii) Mengambil tindakan pengolahan dan kawalan risiko.

A.8.6.2 Sekatan ke atas Pemasangan Perisian (Restriction on Software Installation)

Peranan: Pentadbir Sistem ICT, warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU.

(ii) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa; dan

(iii) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.

A.8.7 Pertimbangan Tentang Audit Sistem Maklumat (Information Systems Audit Considerations)

Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.

A.8.7.1 Kawalan Audit Sistem Maklumat (Information Systems Audit Controls)

Peranan: ICTSO, dan Pentadbir Sistem ICT

Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perniagaan.

BIDANG A.9 : KESELAMATAN KOMUNIKASI (COMMUNICATIONS SECURITY)

A.9.1 Pengurusan Keselamatan Rangkaian (Network Security Management)

Objektif: Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

A.9.1.1 Kawalan Rangkaian (Network Control)

Peranan: Pengarah Bahagan dan Pentadbir Sistem ICT

Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan;

(ii) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk;

(iii) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;

(iv) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;

(v) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian;

(vi) Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan MAMPU;

(vii) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna **KECUALI** mendapat kebenaran daripada Pegawai Keselamatan Teknologi Maklumat (ICTSO);

(viii) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat MAMPU;

(ix) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

(x) Sebarang penyambungan rangkaian yang bukan di bawah kawalan STM MAMPU adalah tidak dibenarkan;

(xi) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di MAMPU sahaja dan penggunaan modem adalah dilarang sama sekali;

(xii) Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya;

(xiii) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan;

(xiv) Menempatkan atau memasang antara muka (interfaces) yang bersesuaian di antara rangkaian MAMPU, rangkaian agensi lain dan rangkaian awam;

(xv) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;

(xvi) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja;

(xvii) Mengawal capaian fizikal dan logikal ke atas kemudahan *port* diagnostik dan konfigurasi jarak jauh;

(xviii) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan MAMPU; dan

(xix) Mewujud dan melaksana kawalan pengalihan laluan (routing control) bagi memastikan pematuhan terhadap peraturan MAMPU.

A.9.1.2 Keselamatan Perkhidmatan Rangkaian (Security of Network Services)

Peranan: ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT dan Pembekal

Pengurusan bagi semua perkhidmatan rangkaian (inhouse atau outsource) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.

A.9.1.3 Pengasingan Dalam Rangkaian (Segregation in Networks)

Peranan: ICTSO, Pengarah Bahagian dan Pentadbir Sistem ICT

Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian MAMPU.

A.9.2 Pemindahan Data dan Maklumat (Information Transfer)

Objektif: Memastikan keselamatan perpindahan/pertukaran data maklumat dan perisian antara MAMPU dan pihak luar terjamin.

A.9.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat (Information Transfer Policies and Procedures)

Peranan: Pengguna, warga MAMPU dan pembekal

Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi;

(ii) Terma pemindahan data, maklumat dan perisian antara MAMPU dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;

(iii) Media yang mengandungi maklumat perlu dilindungi; dan

(iv) Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.

A.9.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat (Agreements on Information Transfer)

Peranan: CIO dan Pengarah Bahagian

MAMPU perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara MAMPU dengan pihak luar. Perkara yang perlu dipertimbangkan ialah:

(i) Pengarah Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat MAMPU;

(ii) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat MAMPU;

(iii) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan

(iv) MAMPU hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.

A.9.2.3 Pesanan Elektronik (Electronic Messaging)

Peranan: Warga MAMPU

Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti **LAMPIRAN B**:

(i) Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003;

(ii) Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 – Pematuhan Tatacara Penggunaan E-mel dan Internet;

(iii) Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkah-langkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan

(iv) Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa; dan

(v) Sebarang e-mel rasmi hendaklah direkod ke dalam DDMS 2.0 untuk tujuan rekod.

A.9.2.4 Perjanjian Kerahsiaan atau Ketakdedahan (Confidentiality Or Non-Disclosure Agreements)

Peranan: ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT, Pengguna dan Pembekal

Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan.

Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.

BIDANG A.10 : PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM (SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE)

A.10.1 Keperluan Keselamatan Sistem Maklumat (Security Requirements of Information Systems)

Objektif: Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang seluruh kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan dalam rangkaian awam.

A.10.1.1 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat (Information Security Requirements Analysis And Spesifications)

Peranan: Pentadbir Sistem ICT

Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut:

(i) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan;

(ii) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber MAMPU;

(iii) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan

(iv) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.

A.10.1.2 Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam (Securing Application Services on Public Networks)

Peranan: Pentadbir Sistem ICT

Perkara yang perlu dipertimbangkan adalah seperti berikut:

(i) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi MAMPU. Contoh perkhidmatan sumber luaran ialah:

(a) Perisian Sebagai Satu Perkhidmatan;

(b) Platform Sebagai Satu Perkhidmatan;

(c) Infrastruktur Sebagai Satu Perkhidmatan;

(d) Storan Pengkomputeran Awan; dan

(e) Pemantauan Keselamatan.

(ii) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;

(iii) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (authentication);

(iv) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;

(v) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan

(vi) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.

A.10.1.3 Melindungi Transaksi Perkhidmatan Aplikasi (Protecting Application Services Transactions)

Peranan: ICTSO, Pengarah Bahagian dan Pentadbir Sistem ICT

Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;

(ii) Memastikan semua aspek transaksi dipatuhi:

(a) maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan;

(b) mengekalkan kerahsiaan maklumat;

(c) mengekalkan privasi pihak yang terlibat; dan

(d) protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi.

(iii) Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.

A.10.2 Keselamatan Dalam Proses Pembangunan dan Sokongan (Security in Development and Support Services)

Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

A.10.2.1 Dasar Pembangunan Selamat (Secure Development Policy)

Peranan: ICTSO, Pengarah Bahagian dan Pentadbir Sistem ICT

Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Keselamatan persekitaran pembangunan;

(ii) Keselamatan pangkalan data;

(iii) Keperluan keselamatan dalam fasa reka bentuk;

(iv) Keperluan *check point* keselamatan dalam carta perbatuan projek;

(v) Keperluan pengetahuan ke atas keselamatan aplikasi;

(vi) Keselamatan dalam kawalan versi; dan

(vii) Bagi pembangunan secara penyumberluaran (outsource), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.

A.10.2.2 Prosedur Kawalan Perubahan Sistem (System Change Control Procedures)

Peranan: Pengarah Bahagian dan Pentadbir Sistem ICT

Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;

(ii) aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;

(iii) mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan

(iv) capaian kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.

A.10.2.3 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi (Technical Review Of Applications After Operating Platform Changes)

Peranan: Pentadbir Sistem ICT

Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform.

(ii) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan

(iii) Memastikan perubahan yang sesuai dibuat kepada PKP MAMPU dan Pelan Pemulihan Bencana Sistem yang berkaitan berdasarkan Pelan Pengurusan Keselamatan Maklumat (ISMP) sistem tersebut.

A.10.2.4 Sekatan Ke atas Perubahan Dalam Pakej Perisian (Restrictions on Changes to Software Packages)

Peranan: Pentadbir Sistem ICT, Pengarah Bahagian

Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.

A.10.2.5 Prinsip Kejuruteraan Sistem Yang Selamat (Secure System Engineering Principles)

Peranan: Pentadbir Sistem ICT, Pengarah Bahagian

Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada **Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V)** sektor awam yang terkini.

A.10.2.6 Persekitaran Pembangunan Selamat (Secure Development Environment)

Peranan: Pentadbir Sistem ICT dan Pengarah Bahagian

Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.

MAMPU perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:

(i) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;

(ii) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;

(iii) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;

(iv) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;

(v) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan

(vi) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.

A.10.2.7 Pembangunan oleh Khidmat Luaran (Outsourced Software Development)

Peranan: Pentadbir Sistem ICT, Pengarah Bahagian, ICTSO

MAMPU hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (source code) adalah menjadi **HAK MILIK** MAMPU. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Perkiraan perlesenan, kod sumber ialah **HAK MILIK** MAMPU dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*;

(ii) Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori **"Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko"**;

(iii) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik;

(iv) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;

(v) Mengguna pakai prinsip dan tatacara ***escrow***; dan

(vi) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.

A.10.2.8 Pengujian Keselamatan Sistem (System Security Testing)

Peranan: Pentadbir Sistem ICT, ICTSO

Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;

(ii) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan

(iii) menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.

Maklumat lanjut berkaitan pengujian keselamatan sistem boleh merujuk kepada dokumen **ISO/IEC/IEEE 29119 *Software Testing Standard***.

A.10.2.9 Pengujian Penerimaan Sistem (System Accepting Testing)

Peranan: Pengguna, Pentadbir Sistem ICT, ICTSO

Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat (rujuk A.14.1.1 dan A.14.1.2) dan kepatuhan kepada Polisi Pembangunan Selamat (rujuk A.14.2.1);

(ii) penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan

(iii) pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (vulnerability scanner).

Maklumat lanjut berkaitan boleh merujuk kepada dokumen **ISO/IEC/IEEE 29119** ***Software Testing Standard.***

A.10.3 Data Ujian (Test Data)

Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian.

A.10.3.1 Perlindungan Data Ujian (Protection of Test Data)

Peranan: Pengguna, Pentadbir Sistem ICT, ICTSO

Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian;

(ii) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian;

(iii) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan

(iv) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.

BIDANG A.11 : HUBUNGAN PEMBEKAL (SUPPLIER RELATIONSHIP)

A.11.1 Keselamatan Maklumat Dalam Hubungan Pembekal (Information Security in Supplier Relationships)

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

A.11.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal (Information Security Policy for Supplier Relationships)

Peranan: Pengarah Bahagian, Pemilik Projek dan Pembekal

Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset MAMPU. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori;

(ii) Proses kitaran hayat (lifecycle) yang seragam untuk menguruskan pembekal;

(iii) Mengawal dan memantau akses pembekal;

(iv) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;

(v) Jenis-jenis obligasi kepada pembekal;

(vi) Pelan kontigensi (contingency plan) bagi memastikan ketersediaan kemudahan pemprosesan maklumat;

(vii) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber MAMPU kepada pembekal;

(viii) Menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber MAMPU (LAMPIRAN C)**; dan

(ix) Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.

A.11.1.2 Menangani Keselamatan Dalam Perjanjian Pembekal (Addressing Security Within Supplier Agreements)

Peranan: Syarikat Pembekal

Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak MAMPU selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.

Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) MAMPU hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan;

(ii) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan;

(iii) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan;

(iv) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;

(v) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;

(vi) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut:

(a) Badan penilai pihak ketiga adalah bebas dan berintegriti;

(b) Badan penilai pihak ketiga adalah kompeten;

(c) Kriteria penilaian;

(d) Parameter pengujian; dan

(e) Andaian yang dibuat berkaitan dengan skop penilaian.

(vii) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan MAMPU; dan

(viii) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh MAMPU.

A.11.1.3 Rantaian Bekalan Teknologi Maklumat dan Komunikasi (Information and Communication Technology Supply Chain)

Peranan: Pengarah Bahagian, Pembekal dan Pemilik Projek

Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:

(i) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;

(ii) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan

(iii) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.

A.11.2 Pengurusan Penyampaian Perkhidmatan Pembekal (Supplier Service Delivery Management)

Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.

A.11.2.1 Memantau dan Mengkaji Semula Perkhidmatan Pembekal (Monitoring and Review Supplier Services)

Peranan: Pengarah Bahagian, Pembekal dan Pemilik Projek

MAMPU hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:

(i) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan;

(ii) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan

(iii) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.

A.11.2.2 Menguruskan Perubahan Kepada Perkhidmatan Pembekal (Managing Changes to Supplier Services)

Peranan: Pengarah Bahagian, Pembekal dan Pemilik Projek

Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut:

(i) Perubahan dalam perjanjian dengan pembekal;

(ii) Perubahan yang dilakukan oleh MAMPU bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan

(iii) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.

BIDANG A.12 : PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT (INFORMATION SECURITY INCIDENT MANAGEMENT)

A.12.1 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan (Management of Information Security Incidents and Improvements)

Objektif: Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan.

A.12.1.1 Tanggungjawab dan Prosedur (Responsibilities and Procedures)

Peranan: ICTSO, Pengarah Bahagian, CERT MAMPU dan Pemilik Projek/Sistem Aplikasi

Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden MAMPU adalah berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CERT MAMPU yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Memberikan kesedaran berkaitan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CERT MAMPU dan hebahan kepada warga MAMPU sekiranya ada perubahan; dan

(ii) Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

A.12.1.2 Pelaporan Kejadian Keselamatan Maklumat (Reporting Information Security Events)

Peranan: ICTSO, Pengarah Bahagian dan CERT MAMPU

Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CERT MAMPU. CERT MAMPU kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa;

(ii) Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa;

(iii) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

(iv) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;

(v) Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan;

(vi) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

(vii) Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.

Prosedur pelaporan insiden keselamatan siber berdasarkan:

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

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

(iii) Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CERT MAMPU

A.12.1.3 Pelaporan Kelemahan Keselamatan Maklumat (Reporting Security Weaknesses)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Warga MAMPU dan pembekal yang menggunakan sistem dan perkhidmatan maklumat MAMPU dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.

A.12.1.4 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat (Assessment of and Decision on Information Security Events)

Peranan: ICTSO

Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.

A.12.1.5 Tindak Balas Terhadap Insiden Keselamatan Maklumat (Response to Information Security Incidents)

Peranan: ICTSO, CERT MAMPU

Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan **Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CERT MAMPU.**

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

(i) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;

(ii) Menjalankan kajian forensik sekiranya perlu;

(iii) Menghubungi pihak yang berkenaan dengan secepat mungkin;

(iv) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti;

(v) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;

(vi) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;

(vii) Menyediakan tindakan pemulihan segera; dan

(viii) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.

A.12.1.6 Pembelajaran Daripada Insiden Keselamatan Maklumat (Learning from Information Security Incidents)

Peranan: ICTSO, CERT MAMPU

Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya.

Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.

A.12.1.7 Pengumpulan Bahan Bukti (Collection of Evidence)

Peranan: ICTSO, CERT MAMPU

MAMPU hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.

BIDANG A.13: ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT)

A.13.1 Kesinambungan Keselamatan Maklumat (Information Security Continuity)

Objektif: Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan bisnes MAMPU.

A.13.1.1 Perancangan Kesinambungan Keselamatan Maklumat (Planning Information Security Continuity)

Peranan: Koordinator PKP, Pasukan Tindak balas Kesemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT

MAMPU hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, MAMPU perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi MAMPU.

MAMPU juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) MAMPU;

(ii) Menetapkan polisi PKP;

(iii) Mengenal pasti perkhidmatan kritikal;

(iv) Melaksanakan Kajian Impak Perkhidmatan (Business Impact Analysis – BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal;

(v) Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT.

(vi) Melaksanakan program kesedaran dan latihan pasukan PKP dan warga MAMPU;

(vii) Melaksanakan simulasi ke atas dokumen di para (c); dan

(viii) Melaksanakan penyelenggaraan ke atas pelan di para (c).

A.13.1.2 Pelaksanaan Kesinambungan Keselamatan Maklumat (Implementing Information Security Continuity)

Peranan: Koordinator PKP, Pasukan Tindak balas Kesemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT

MAMPU hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal MAMPU yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini;

(ii) Melaksanakan *post-mortem* dan mengemaskini pelan-pelan PKP;

(iii) Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal MAMPU;

(iv) Mengemas kini struktur tadbir urus PKP MAMPU jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan

(v) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.

A.13.1.3 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat (Verify, Review and Evaluate Information Security Continuity)

Peranan: Pengurusan Atasan MAMPU, Koordinator PKP, Pasukan Tindak balas Kesemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT, Pemilik Perkhidmatan Kritikal MAMPU dalam PKP dan warga MAMPU

MAMPU hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.

A.13.2 Lewahan (Redundancy)

Objektif: Untuk memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.

A.13.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat (Availability of Information Process Facilities)

Peranan: Pentadbir Pusat Data, Pemilik Perkhidmatan dan Pentadbir Sistem ICT

Kemudahan pemprosesan maklumat MAMPU perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (failover test) keberkesanannya dari semasa ke semasa.

BIDANG A.14: PEMATUHAN (COMPLIANCE)

A.14.1 Pematuhan Terhadap Keperluan Perundangan dan Kontrak (Compliance with Legal and Contractual Requirements)

Objektif: Meningkat dan memantapkan tahap keselamatan siber bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

A.14.1.1 Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai (Identification of Applicable Legislation and Contractual Agreement)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MAMPU dan pembekal seperti **LAMPIRAN B.**

A.14.1.2 Hak Harta Intelek (Intellectual Property Rights)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.

A.14.1.3 Perlindungan Rekod (Protection of Records)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.

A.14.1.4 Privasi dan Perlindungan Maklumat Peribadi (Privacy and Protection of Personally Identifiable Information)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

MAMPU hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.

A.14.1.5 Peraturan Kawalan Kriptografi (Regulation of Cryptographic Controls)

Peranan: Warga MAMPU, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MAMPU

A.14.2 Kajian Semula Keselamatan Maklumat (Information Security Reviews)

Objektif: Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur MAMPU.

A.14.2.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali (Independent Review of Information Security)

Peranan: Pengarah Bahagian dan Pemilik Perkhidmatan

Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.

A.14.2.2 Pematuhan Polisi dan Standard Keselamatan (Compliance with Security Policies and Standards)

Peranan: Pengarah Bahagian dan Pemilik Perkhidmatan

MAMPU hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.

A.14.2.3 Kajian Semula Pematuhan Teknikal (Technical Compliance Review)

Peranan: Pengarah Bahagian dan Pemilik Perkhidmatan

MAMPU hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.

LAMPIRAN B

UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Arahan Pentadbiran Ketua Pengarah MAMPU Bilangan 1 Tahun 2019 ini hendaklah dibaca bersama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuatkuasa antaranya seperti berikut;

1. Arahan Keselamatan;
2. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";
3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
4. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";
6. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
7. Surat Pekeliling Am Bil. 4 Tahun 2006 – "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";
8. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- "Tatacara Penyediaan, Penilaian dan PenerimaanTender";
9. Surat Pekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan";
10. Akta Tandatangan Digital 1997;

11. Akta Rahsia Rasmi 1972;
12. Akta Jenayah Komputer 1997;
13. Akta Hak Cipta (Pindaan) Tahun 1997;
14. Akta Komunikasi dan Multimedia 1998;
15. Perintah-Perintah Am;
16. Arahan Perbendaharaan;
17. Arahan Teknologi Maklumat 2007;
18. Standard Operating Procedure (SOP) ICT MAMPU;
19. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";
20. Etika Penggunaan E-mel dan Internet MAMPU;
21. Surat Akujanji;
22. Myportfolio;
23. Pelan Kesinambungan Perkhidmatan;
24. Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk "Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan";
25. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk "Penggunaan Media Jaringan Sosial di Sektor Awam";
26. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)";
27. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam;
28. Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007";

29. Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT MAMPU;

30. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;

31. Garis Panduan GPKI ; dan

32. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 "Langkah-langkah mengenai penggunaan Mel Elektronik Agensi – Agensi Kerajaan", Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC).

LAMPIRAN C

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER MAMPU

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

.....

( )

b.p. Ketua Pengarah MAMPU

Tarikh: