SURUHANJAYA INTEGRITI AGENSI PENGUATKUASAAN

POLISI KESELAMATAN SIBER

SURUHANJAYA INTEGRITI AGENSI PENGUATKUASAAN

VERSI 1.1

2023

ISI KANDUNGAN

TAKRIFAN

Bagi maksud pemakaian Polisi Keselamatan Siber EAIC ini, arahan yang dipakai adalah berpandukan Arahan Pentadbiran Ketua Pengarah MAMPU Bil 4 Tahun 2020 dengan takrifan berikut:

(1)	Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita *magnetic, 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)	BCP/PKP	*Business Continuity Planning* Pelan Kesinambungan Perkhidmatan
(6)	CCTV	*Closed-Circuit Televison System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
(7)	CIO	*Chief Information Officer*

		Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi
(8)	*Clear Desk & 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.
(9)	CSIRT EAIC	*Cyber Security Incident Response Team (CSIRT)* EAIC atau Pasukan Tindak Balas Insiden Keselamatan Siber EAIC
(10)	*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 travelling to system endpoints, such as mobile devices or workstations.*
(11)	*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.*
(12)	*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.*
(13)	*Denial of service*	Halangan pemberian perkhidmatan.

(14)	*Defence-in-depth*	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
(15)	*Encryption*	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
(16)	*Escrow* (eskrow)	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
(17)	*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.
(18)	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
(19)	ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
(20)	ICTSO	ICT *Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
(21)	Insiden keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau kemungkinan berlaku kejadian tersebut.

(22)	*Internet*	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
(23)	*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.
(24)	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
(25)	*Instrusion 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.
(26)	*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.

(27)	MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
(28)	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
(29)	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data maklumat.
(30)	LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer
(31)	*Lock*	Mengunci komputer
(32)	*Logout*	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
(33)	*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.
(34)	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.
(35)	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
(36)	Pasukan ERT	Pasukan Tindakan Kecemasan/Emergency Response Team (ERT)
(37)	Pasukan Projek	Pasukan yang terdiri daripada satu atau lebih kumpulan yang akan memberi fokus kepada bidang teknikal dan bisnes mengikut keperluan dan kesesuaian projek.
(38)	Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
(39)	Pemilik perkhidmatan digital/ projek/sistem	Pemilik kepada perkhidmatan yang dikawal selia oleh sesuatu bahagian/unit atau Pihak yang akan menerima projek setelah projek tersebut disiapkan dan bertanggungjawab ke atas hampir keseluruhan projek dari aspek bisnes.

(40)	Pengarah Bahagian	Bertanggungjawab melaksanakan hal ehwal pengurusan dan pembangunan organisasi di bahagian
(41)	Pengarah BKP (Bahagian Khidmat Pengurusan)	Bertanggungjawab melaksanakan hal ehwal pengurusan dan pentadbiran di BKP EAIC
(42)	Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksanakan berdasarkan hasil penilaian risiko.
(43)	Pengguna	Merujuk kepada warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC.
(44)	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.
(45)	Polisi Keselamatan Maklumat	Satu set polisi yang dikeluarkan oleh EAIC untuk memastikan bahawa semua pengguna teknologi maklumat dalam domain organisasi atau rangkaiannya mematuhi peraturan dan garis panduan yang berkaitan dengan keselamatan maklumat
(46)	*Public-Key Infrastructure* (PKI)	Infastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi

		melindungi keselamatan berkomunikasi dan transaksi melalui internet.
(47)	*Rollback* (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
(48)	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian internet.
(49)	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.
(50)	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ia tidak digunakan dalam jangka masa tertentu.
(51)	*Server*	Pelayan komputer
(52)	*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.

(53)	*Switch*	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.
(54)	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
(55)	*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.
(56)	Virus	Atur cara yang bertujuan merosakkan data atau aplikasi sistem aplikasi.
(57)	WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.
(58)	Warga EAIC	Kakitangan yang berkhidmat di EAIC sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT EAIC.
(59)	*Wireless* LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

(60)	*Worm*	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

TUJUAN

Polisi Keselamatan Siber Suruhanjaya Integriti Agensi Penguatkuasaan (EAIC) ini bertujuan untuk menerangkan tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC dalam melindungi maklumat di ruang siber.

LATAR BELAKANG

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

OBJEKTIF

Objektif utama Polisi Keselamatan Siber EAIC dibangunkan adalah seperti berikut:

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

(b) Memastikan keselamatan penyampaian perkhidmatan EAIC di tahap tertinggi sekaligus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

(c) Memastikan kelancaran operasi EAIC dengan meminimumkan kerosakan atau kemusnahan disebabkan insiden yang berlaku;

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

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

PENYATAAN POLISI KESELAMATAN SIBER EAIC

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

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:

(a) Kerahsiaan – maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran;

(b) Kesahihan – Data dan maklumat hendaklah dijamin kesahihannya;

(c) Integriti – Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(d) Tidak boleh disangkal – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal; dan

(e) Ketersediaan – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP POLISI

Ruang siber ditakrifkan sebagai sistem-sistem ICT, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem secara fizikal atau maya, serta persekitaran fizikal sistem-sistem tersebut disimpan. Maklumat yang dipindahkan dari ruang siber ke ruang fizikal (melalui cetakan, salinan tulisan tangan serta rakaman foto menggunakan peralatan fotografik) adalah di luar skop polisi ini dan hendaklah ditangani dengan peraturan sedia ada.

Keselamatan siber adalah bermaksud keadaan bagi segala urusan menyedia dan membekalkan perkhidmatan digital yang berasaskan sistem ICT berjalan secara berterusan.

Aset ICT terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Polisi Keselamatan Siber EAIC telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

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

2) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan EAIC, perkhidmatan dan masyarakat.

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

1. **Perkakasan dan peranti fizikal**

   Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan EAIC. Contoh peralatan dan periferal seperti komputer, pelayan, *firewall*, pencetak, peralatan media, peralatan komunikasi dan alat-alat prasarana seperti *Uninterruptible Power Supply (UPS)* dan sebagainya;

2. **Perisian**

   Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada EAIC;

3. **Perkhidmatan**

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

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

4. **Data dan maklumat**

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

5. **Manusia**

   Semua pengguna infrastruktur EAIC yang dibenarkan, termasuk Warga EAIC, pengguna dan pembekal. Individu yang mempunyai pengetahuan untuk melaksanakan skop kerja harian EAIC bagi mencapai misi dan objektif jabatan.

Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan;

6. **Premis Komputer dan Komunikasi**

   Semua kemudahan serta premis yang digunakan untuk menempatkan Perkara 1 hingga 5 di atas. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber EAIC dan perlu dipatuhi adalah seperti berikut:

1. **Akses Atas Dasar Perlu Mengetahui**

   Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut;

2. **Hak Akses Minimum**

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

3. **Kebertanggungjawaban / Akauntabiliti**

   Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Bagi menentukan tanggungjawab

ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

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

4. Pengasingan

Tugas mewujud, menghapus, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (*unauthorized access*) serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

5. Pengauditan

Tujuan aktiviti ini ialah untuk mengenalpasti insiden berkaitan keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, semua aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan

keselamatan atau Jejak audit (*audit trail*). Semua log yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit;

6. Pematuhan

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

7. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan dan ketidakbolehcapaian. Pemulihan boleh dilakukan melalui proses penduaan (backup) dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan (BRP); dan

8. Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

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

EAIC hendaklah melaksanakan penilaian risiko Keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-

langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

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

EAIC perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko yang berlaku dan memilih tindakan berikut: -

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

BIDANG 01 POLISI KESELAMATAN MAKLUMAT	
0101 Hala Tuju Pengurusan Untuk Keselamatan Maklumat	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan EAIC dan perundangan yang berkaitan.	
010101 Polisi Keselamatan Maklumat	
Pelaksanaan polisi ini akan dijalankan oleh Setiausaha EAIC selaku Pengerusi Jawatankuasa Keselamatan ICT (JKICT) EAIC. JKICT ini terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), Pegawai Teknologi Maklumat, Pentadbir Sistem ICT dan semua Pengarah Bahagian. Polisi Keselamatan Siber EAIC mestilah dipatuhi oleh semua warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan EAIC kepada warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC.	JKICT/CIO/ ICTSO/ Pengarah Bahagian

010102 Kajian Semula Polisi Keselamatan Maklumat	
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 EAIC: i) Mengenal pasti dan menentukan perubahan yang diperlukan; ii) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada JKICT bagi tujuan pengesahan; iii) Memaklumkan pindaan yang telah disahkan oleh JKICT kepada warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC; dan iv) Polisi ini hendaklah dikaji semula setiap **LIMA (5) TAHUN SEKALI** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	JKICT/CIO/ ICTSO

BIDANG 02 **PERANCANGAN BAGI KESELAMATAN ORGANISASI**	
0201 Perancangan Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber EAIC.	
020101 Peranan dan Tanggungjawab Keselamatan Maklumat	
(i) Setiausaha EAIC	
Setiausaha EAIC adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: (a) Memastikan penguatkuasaan pelaksanaan Polisi ini; (b) Memastikan warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC memahami dan mematuhi peruntukan – peruntukan di bawah Polisi ini; (c) Memastikan semua keperluan EAIC (sumber kewangan, sumber manusia 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.	Setiausaha EAIC

(ii) Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) bagi EAIC ialah Pengarah Bahagian Khidmat Pengurusan (BKP). Peranan dan tanggungjawab CIO adalah seperti berikut: (a) Membantu Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam Polisi ini; (b) Memastikan kawalan keselamatan maklumat dalam EAIC diseragam dan diselaraskan dengan sebaiknya; (c) Memastikan Pelan Strategik Pendigitalan EAIC mengandungi aspek keselamatan siber; dan (d) Menyelaras pelan latihan dan program kesedaran keselamatan siber.	CIO
(iii) Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi EAIC ialah Pegawai Teknologi Maklumat. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: i) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; ii) Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; iii) Menyedia dan menyebarkan amaran – amaran yang sesuai terhadap kemungkinan berlakunya ancaman	ICTSO

keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah – langkah perlindungan yang bersesuaian; iv) Melaporkan insiden keselamatan siber kepada CSIRT EAIC dan seterusnya membantu dalam penyiasatan atau pemulihan; v) Melaporkan insiden keselamatan siber kepada CIO bagi insiden yang memerlukan Pemulihan Bencana; vi) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; vii) Melaksanakan pematuhan Polisi ini oleh Warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC; viii) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; dan. ix) Menyediakan dan merangka latihan dan program kesedaran keselamatan siber.	
(iv) Pengarah Bahagian	
Peranan dan tanggungjawab Pengarah Bahagian ialah melaksanakan keperluan Polisi ini dalam operasi semasa seperti yang berikut: (a) Perancangan penggunaan sistem atau aplikasi baharu di bahagian sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; (b) Perancangan keperluan pembelian atau peningkatan perisian dan sistem komputer jika diperlukan di bahagian; (c) Perancangan perolehan teknologi dan perkhidmatan komunikasi baru jika diperlukan di bahagian;	Pengarah Bahagian

(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 di bahagian.	
(v) 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.	Pentadbir Sistem ICT
(vi) *Cyber Security Incident Response Team (CSIRT)* EAIC	
CSIRT EAIC terdiri daripada pegawai dan kakitangan Seksyen Teknologi Maklumat (STM) EAIC.	CSIRT EAIC

Peranan dan tanggungjawab CSIRT EAIC 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 ICT/Pelayan untuk mengambil tindakan pemulihan dan pengukuhan; dan e. Menyebarkan makluman berkaitan pengukuhan keselamatan siber kepada Pentadbir Sistem ICT.	
(vii) Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti yang berikut: a. Membaca, memahami dan mematuhi Polisi ini; b. Mengetahui dan memahami implikasi keselamatan siber dan kesan dari tindakannya; c. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d. Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat EAIC; e. Melaksanakan langkah – langkah perlindungan seperti yang berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia digunakan; iv. Menjaga kerahsiaan maklumat;	Pengguna

v. Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan; vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT EAIC dengan segera; g. Menghadiri program – program kesedaran mengenai keselamatan siber; dan h. Bersetuju dengan terma dan syarat yang terkandung dalam Polisi ini.	
020102 Pengasingan Tugas	
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	Pengarah Bahagian/Pentadbir Sistem ICT

serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan; iii. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara 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.	
020103 Hubungan Dengan Pihak Berkuasa	
Hubungan yang baik dengan pihak berkuasa hendaklah dikekalkan. Perkara – perkara yang perlu dipatuhi adalah seperti yang berikut; a) hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab EAIC; b) mewujud dan mengemaskini 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 kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan c) insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	BKP, CSIRT EAIC

020104 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus	
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau 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 berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Seksyen Teknologi Maklumat
020105 Keselamatan Maklumat dalam Pengurusan 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 EAIC; b. Objektif keselamatan maklumat hendaklah dikendalikan dan 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	Warga EAIC (Pasukan Projek)

yang terkandung dalam Polisi Keselamatan Siber EAIC; dan e. Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.	

0202 Peranti Mudah Alih Dan Telekerja

Objektif:
Memastikan keselamatan telekerja dan penggunaan peralatan mudah alih

020201 Polisi Peranti Mudah Alih

Membangun serta menyebarkan dasar dan langkah – langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih.	Sokongan Teknikal EAIC (STM)
Meluluskan dasar, arahan, peraturan keselamatan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga EAIC.	JKICT EAIC
Perkara – perkara yang perlu dipatuhi: i. Pendaftaran ke atas peralatan mudah alih; ii. Keperluan ke atas perlindungan secara fizikal; iii. Kawalan ke atas pemasangan perisian peralatan mudah alih; iv. Kawalan ke atas versi dan *patches* perisian; v. Sekatan ke atas akses perkhidmatan maklumat secara dalam talian; vi. Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan	Warga EAIC

vii. Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.	
020202 Telekerja	
Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja.	Warga EAIC

BIDANG 3

KESELAMATAN SUMBER MANUSIA

0301 Sebelum Perkhidmatan

Objektif:

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

030101 Tapisan Keselamatan

Tapisan keselamatan hendaklah dijalankan terhadap warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dan perkhidmatan ICT EAIC 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 EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan ii. Menjalankan tapisan keselamatan untuk warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Pengguna

030102 Terma dan Syarat Perkhidmatan	
Persetujuan berkontrak dengan warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC 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 EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC 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.	Pengguna
0302 Dalam Tempoh Perkhidmatan	
Objektif: Memastikan warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC 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.	
030201 Tanggungjawab Pengurusan	
Pengurusan hendaklah memastikan warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT	Pengguna

EAIC mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	
030202 Kesedaran, Pendidikan dan Latihan tentang Keselamatan Maklumat	
Warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC 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 berikut: i. Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber EAIC 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 EAIC 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.	Pengguna
030203 Proses Tatatertib	
Proses tatatertib yang formal dan disampaikan kepada warga EAIC hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga EAIC yang melakukan pelanggaran keselamatan maklumat.	BKP
0303 Penamatan dan Pertukaran Perkhidmatan	

Objektif: Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas warga EAIC diurus dengan teratur.	
030301 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan	
Warga EAIC yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut: a. Memastikan semua aset ICT dikembalikan kepada EAIC mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan EAIC dan/atau terma perkhidmatan yang ditetapkan. c. Maklumat rasmi EAIC dalam peranti tidak dibenarkan dibawa keluar dari EAIC.	STM dan Warga EAIC
Warga EAIC yang telah bertukar perkhidmatan hendaklah: a. memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada EAIC mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b. menyediakan dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	STM dan Warga EAIC

BIDANG 4

PENGURUSAN ASET

0401 Tanggungjawab Terhadap Aset

Objektif:

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

040101 Inventori Aset

Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT EAIC. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a. EAIC hendaklah mengenal pasti Pegawai Penerima Aset setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT; b. Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemaskini sebagaimana arahan dan peraturan yang berkuatkuasa dari semasa ke semasa; c. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan d. Pegawai Aset hendaklah mengesahkan penempatan aset ICT.	Pegawai Penerima Aset, Pegawai Aset dan Warga EAIC

040102 Pemilikan Aset

Aset yang diselenggara adalah hak milik EAIC. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara – perkara berikut:	Pegawai Aset dan Warga EAIC

a. Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; b. Memastikan aset telah dikelaskan dan dilindungi; c. Kenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; d. Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan e. Memastikan semua jenis aset dipelihara dengan baik.	
040103 Penggunaan Aset yang Dibenarkan	
Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	Warga EAIC
040104 Pemulangan Aset	
Warga EAIC hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	Warga EAIC
0402 Pengelasan Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	

040201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.	Pegawai Pengelasan
040202 Pelabelan Maklumat	
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.	Warga EAIC
040203 Pengendalian Aset	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan tersebut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa dan menentukan maklumat adalah 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, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan siber daripada ketahui umum	Warga EAIC

0403 Pengendalian Media	
Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan**.**	
040301 Pengurusan Media	
Prosedur pengurusan media hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh EAIC. Prosedur – prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal rekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan e. Menyimpan semua jenis media di tempat yang selamat.	Pengguna
040302 Pelupusan Media	
a. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan. b. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pegawai Aset dan Jawatankuasa yang dilantik untuk pelupusan aset/Pentadbir Sistem ICT

BIDANG 5

KAWALAN AKSES

0501 Kawalan Akses

Objektif:

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

050101 Polisi Kawalan Akses

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 dikemaskini 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 berkuatkuasa semasa; iv. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;	Pemilik perkhidmatan digital dan Pentadbir Sistem ICT

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.*	
050102 Capaian kepada Rangkaian dan Perkhidmatan Rangkaian	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari EAIC. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: i. Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian EAIC, 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.	ICTSO dan Pentadbir Rangkaian/Pentadbir Sistem ICT
0502 Pengurusan Akses Pengguna	
Objektif: Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada.	

050201 Pendaftaran dan Pembatalan Pengguna	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses dilakukan. Perkara – perkara berikut hendaklah dipatuhi: i. Akaun yang diperuntukkan oleh EAIC sahaja boleh digunakan; ii. Akaun pengguna mestilah unik; iii. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada EAIC 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 EAIC.	Warga EAIC/Pentadbir Sistem ICT/Pentadbir E-mel
050202 Peruntukan Akses Pengguna	
Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.	STM
050203 Pengurusan Hak Akses Istimewa	
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 Sistem Aplikasi yang diwujudkan.	Pengguna /Pentadbir Sistem ICT

050204 Pengurusan Maklumat Pengesahan Rahsia Pengguna	
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyediaan yang ketat berdasarkan keperluan.	ICTSO dan Pentadbir Sistem ICT
050205 Kajian Semula Hak Akses Pengurusan	
Pentadbir Sistem ICT 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.	ICTSO dan Pentadbir Sistem ICT
050206 Pembatalan atau Pelarasan Hak Akses	
Hak akses Warga EAIC 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 EAIC.	Pentadbir Sistem ICT
0503 Tanggungjawab Pengguna	
Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka	

050301 Penggunaan Maklumat Pengesahan Rahsia	
Pengguna perlu mengikut amalan keselamatan yang. baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.	Pengguna, Pentadbir Sistem, ICTSO, Pengarah Bahagian
0504 Kawalan Akses Sistem dan Aplikasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.	
050401 Sekatan Akses Maklumat	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut - kawalan capaian yang ditetapkan.	Pengguna, Pentadbir Sistem, ICTSO, Pengarah Bahagian
050402 Prosedur Log Masuk Yang Selamat	
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 berikut: a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan EAIC;	Pentadbir Sistem/ICTSO

b. Menjana amaran *(alert)* sekiranya berlaku pelanggaran semasa log masuk terhadap aplikasi sistem; c. Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; d. Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; e. Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan yang berkualiti; dan f. Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
050403 Sistem Pengurusan Kata Laluan	
Sistem pengurusan kata laluan hendaklah interaktif dan mengambil kira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh EAIC seperti yang berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. 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. d. Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun; e. Kata laluan paparan kunci *(lock screen)* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;	Warga EAIC

f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; g. Kuat kuasakan pertukaran kata laluan semasa atau selepas log masuk kali pertama atau selepas reset kata laluan; h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i. 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 diaktif semula; dan j. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
050404 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa	
Penggunaan program utiliti hendaklah dikawal bagi mengelakkan sistem *Over-Riding*.	Pentadbir Sistem ICT
050405 Kawalan Akses Kepada Kod Sumber Program	
Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; (b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan (c) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik EAIC.	Pengarah Projek, Pengurus Projek dan Pentadbir Sistem ICT

BIDANG 6 **KRIPTOGRAFI**	
0601 Kawalan Kriptografi	
Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan dan / atau keutuhan maklumat	
060101 Polisi Penggunaan Kawalan Kriptografi	
Kriptografi merangkumi kaedah-kaedah seperti yang berikut: **i) Enkripsi** Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi *(encryption)* **ii) Tandatangan Digital** Maklumat terperinci yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan.	Pengarah Projek
060102 Pengurusan Kunci Awam	
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	STM, Pengarah BKP

BIDANG 7

KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Kawasan Selamat

Objektif:

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

070101 Perimeter Keselamatan Fizikal

Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan Aset ICT EAIC. 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.	BKP

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.	
070102 Kawalan Kemasukan Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap pengguna EAIC hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan balik kepada EAIC apabila pengguna berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter lobi Bangunan Menara Usahawan. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan segera.	Pengguna
070103 Keselamatan Pejabat, Bilik dan Kemudahan	
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: i. Kawasan tempat bekerja, bilik rahsia, bilik krisis, bilik fail, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; ii. Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan	Pengguna/BKP

iii. Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.	
070104 Perlindungan Daripada Ancaman Luar Dan Persekitaran	
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. EAIC perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	BKP
070105 Bekerja di Kawasan Selamat	
Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga EAIC yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis EAIC termasuklah Pusat Data.	BKP
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 EAIC 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;	BKP

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 berkenaan; 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.	
070106 Kawasan Penyerahan dan Pemunggahan	
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. EAIC hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	BKP
0702 Peralatan ICT	
Objektif: Melindungi peralatan ICT EAIC daripada kehilangan, kerosakan, kecurian dan disalahgunakan.	

070201 Penempatan dan Perlindungan Peralatan ICT

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 ICT; 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, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran. vii) Semua pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan 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 memunyai ciri-ciri keselamatan;	Pengguna

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 guna sama yang hendak dibawa keluar perlukan mendapat kelulusan dan direkodkan bagi tujuan pemantauan;

xiii) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan kehilangan aset/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 peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk untuk dibaik pulih;

xvii) Sebarang pelekat selain 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 EAIC sahaja.

070202 Utiliti Sokongan	
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).	STM/Pentabdir Sistem ICT
070203 Keselamatan Kabel	
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan dan kerosakan. i. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. 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 *wiretapping*; dan v. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pentadbir sistem ICT

070204 Penyelenggaraan Peralatan	
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 perkaksan 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.	STM, Pentadbir sistem ICT
070205 Pengalihan 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 EAIC untuk tujuan rasmi, perlulah mendapat kelulusan pegawai yang diturunkan kuasa dan direkodkan bagi tujuan	Pengguna, Pegawai Aset

pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan ii. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	
070206 Keselamatan Peralatan dan Aset di Luar Premis	
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis EAIC. Peralatan yang dibawa keluar dari premis EAIC 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.	Pengguna
070207 Pelupusan yang Selamat atau Penggunaan Semula Peralatan	
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 EAIC dan ditempatkan di EAIC.	Pegawai Aset, Pentadbir Sistem ICT dan warga EAIC

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 EAIC. Langkah-langkah seperti yang berikut hendaklah diambil:

(a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui shredding, grinding, degaussing atau pembakaran;
(b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;
(c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;
(d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
(e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
(f) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT;
(g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan
(h) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:
    - Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.

- Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM*, *hardisk*, *motherboard* dan sebagainya;
- Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di EAIC;
- Memindah keluar dari EAIC mana-mana peralatan ICT yang hendak dilupuskan; dan
- Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab EAIC.

(i) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti cakera padat, pita magnetik, *optical disk*, *flash disk*, *CDROM*, *thumb drive* dan media storan lain sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

(j) 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;

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

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

(m) Pegawai aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem aset.

070208 Peralatan Pengguna Tanpa Kawalan	
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.	Pengguna
070209 Dasar Meja Kosong dan Skrin Kosong	
Dasar meja kosong untuk kertas dan penyimpanan media 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 *sensitive* 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 screen saver* atau *logout* apabila meninggalkan komputer; ii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;	Warga EAIC

iii.	Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili 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 8

KESELAMATAN OPERASI

0801 Prosedur dan Tanggungjawab Operasi

Objektif:

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

080101 Pengendalian Prosedur

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 didokumen, 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 dikemas kini dari semasa ke semasa atau mengikut keperluan.	BKP, Pentadbir Sistem ICT

080102 Pengurusan Perubahan

Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan	Pentadbir Sistem ICT

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 di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
080103 Pengurusan Kapasiti	
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	STM, Pentadbir Sistem ICT

ii. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	
8.1.4 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi	
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 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.	STM, Pentadbir Sistem ICT
0802 Perlindungan Daripada Perisian Hasad	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*	

080201 Kawalan Daripada Perisian Hasad	
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada 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 berbahaya 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 pattern *antivirus* yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan	Pentadbir Sistem ICT, ICTSO

(i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	

0803 Sandaran

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

080301 Sandaran Maklumat

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: (a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi; (c) Menguji sistem sandaran sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan (d) 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**.	Pentadbir Sistem ICT

0804 Pengelogan dan Pemantauan	
Objektif: Merekodkan peristiwa dan menghasilkan bukti.	
080401 Pengelogan Kejadian	
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.	Pentadbir Sistem ICT
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: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;	

b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada CSIRT EAIC/NACSA.	
080402 Perlindungan Maklumat Log	
Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.	Pentadbir Sistem ICT
080403 Log Pentadbir dan Pengendali	
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 ambil 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	Pentadbir Sistem ICT, CSIRT EAIC

hendaklah melaporkan kepada pasukan CSIRT EAIC/NACSA.	
080404 Penyeragaman Jam	
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 EAIC atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM).	Pentadbir Sistem ICT
0805 Kawalan Perisian yang Beroperasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
080501 Pemasangan Perisian Pada Sistem yang Beroperasi	
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	Pentadbir Sistem ICT

iii. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.	
0806 Pengurusan Kerentanan Teknikal	
Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
080601 Pengurusan Kerentanan Teknikal	
Maklumat tentang kerentanan tenikal 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.	Pentadbir Sistem ICT, CSIRT EAIC

080602 Sekatan ke atas Pemasangan Perisian	
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 EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC; ii. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana- mana undang-undang bertulis yang berkuat kuasa; iii. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	Pentadbir Sistem ICT, Pengguna
0807 Pertimbangan Tentang Audit Sistem Maklumat	
Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.	
080701 Kawalan Audit Sistem Maklumat	
Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perniagaan.	ICTSO dan Pentadbir Sistem ICT

BIDANG 9 **KESELAMATAN KOMUNIKASI**	
0901 Pengurusan Keselamatan Rangkaian	
Objektif: Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.	
090101 Kawalan Rangkaian	
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan rangkaian mestilah melalui proses *Factory Acceptance Check (FAC)* semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT/Rangkaian; (f) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan EAIC; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna KECUALI mendapat kebenaran daripada ICTSO;	STM, Pentadbir Sistem ICT

(h) Memasang perisian Intrusion *Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat EAIC;

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

(j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan STM EAIC adalah tidak dibenarkan;

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

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

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

(n) Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian di antara rangkaian EAIC, rangkaian agensi lain dan rangkaian awam;

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

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

(q) Mengawal capaian fizikal dan logical ke atas kemudahan *port diagnostic* dan konfigurasi jarak jauh;

(r) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan EAIC; dan

(s) Mewujud dan melaksana kawalan pengalihan laluan *(routing control)* bagi memastikan pematuhan terhadap peraturan EAIC.

090102 Keselamatan Perkhidmatan Rangkaian	
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.	ICTSO, Pentadbir Sistem ICT dan Pembekal
090103 Pengasingan Dalam Rangkaian	
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian EAIC.	ICTSO, dan Pentadbir Sistem ICT
0902 Pemindahan Data dan Maklumat	
Objektif: Memastikan keselamatan perpindahan/pertukaran data maklumat dan perisian antara EAIC dan pihak luar terjamin.	
090201 Polisi dan Prosedur Pemindahan Data dan Maklumat	
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 EAIC dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;	Warga EAIC

iii. Media yang mengandungi maklumat perlu dilindungi; dan iv. Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	
090202 Perjanjian Mengenai Pemindahan Data dan Maklumat	
EAIC perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara EAIC dengan pihak luar. Perkara yang perlu dipertimbangkan ialah: i. Pengarah Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat EAIC; ii. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat EAIC; iii. Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan iv. EAIC hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	CIO dan Pengarah Bahagian
090203 Pesanan Elektronik	
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 A:	Warga EAIC

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 Pengguna E-mel dan Internet; iii. Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication* (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa; dan iv. Sebarang e-mel/surat rasmi hendaklah direkod ke dalam DDMS 2.0 untuk tujuan rekod (sekiranya berkaitan).	
090204 Perjanjian Kerahsiaan atau Ketakdedahan	
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan didokumentasikan. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT, Pengguna

BIDANG 10

PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

1001 Keperluan Keselamatan Sistem Maklumat

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.

100101 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat

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 termsuk 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 EAIC; iii. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan	Pentadbir Sistem ICT

iv. Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.	
100102 Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam	
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 EAIC. 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; Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan v. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	Pentabdir Sistem ICT

100103 Melindungi Transaksi Perkhidmatan Aplikasi	
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.	ICTSO, Pengarah Bahagian dan Pentadbir Sistem ICT, Warga EAIC
1002 Keselamatan Dalam Proses Pembangunan dan Sokongan	
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.	

100201 Dasar Pembangunan Selamat	
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.	ICTSO, STM, Pentadbir Sistem ICT
100202 Prosedur Kawalan Perubahan Sistem	
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: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan Pentadbir Sistem ICT aplikasi	STM, Pentadbir Sistem ICT

hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; dan d) capaian kepada kod sumber *(source code)* aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja. e) Mempunyai keupayaan untuk menamatkan aplikasi secara automatik *(auto logoff)* bagi pengguna tidak aktif *(idle)* selepas suatu tempoh masa yang ditetapkan.	
100203 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi	
Apabila platform operasi berubah, aplikasi penting 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.	ICTSO/STM/Pentadbir Sistem ICT

ii. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan iii. Memastikan perubahan yang sesuai dibuat kepada Pelan Pemulihan Bencana Sistem untuk yang berkaitan.	
100204 Sekatan Ke atas Perubahan Dalam Pakej Perisian	
Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	STM, Pentadbir Sistem ICT
100205 Prinsip Kejuruteraan Sistem Yang Selamat	
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.	STM, Pentadbir Sistem ICT,
100206 Persekitaran Pembangunan Selamat	
Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.	STM, Pentadbir Sistem ICT

EAIC 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.	
100207 Pembangunan oleh Khidmat Luaran	
EAIC hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber *(source code)* adalah menjadi **HAK MILIK EAIC**. Perkara yang perlu dipatuhi adalah seperti yang berikut: i. Perkiraan perlesenan, kod sumber ialah **HAK MILIK EAIC** 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	STM, Pentadbir Sistem ICT, dan ICTSO

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 ketapan serahan sistem; v. Mengguna pakai prinsip dan tatacara *escrow*; dan vi. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.	
100208 Pengujian Keselamatan Sistem	
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 **ISO/IEC/IEEE 29119 *Software Testing Standard.***	Pentadbir Sistem ICT, ICTSO
100209 Pengujian Penerimaan Sistem	

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 Bidang 140101 dan 140102) dan kepatuhan kepada Polisi Pembangunan Selamat (rujuk Bidang 140201). 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 kerentanan *(vulnerability scanner).* Maklumat lanjut berkaitan boleh merujuk kepada dokumen **ISO/IEC/IEEE 29119 *Software Testing Standard***.	Pasukan Projek/Pemilik Projek, Pentadbir Sistem ICT, ICTSO
1003 Data Ujian	
Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian.	
100301 Perlindungan Data Ujian	
Data ujian hendaklah dipilih dengan teliti, perkara yang perlu dipatuhi adalah seperti yang berikut: i. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian;	Pengguna, Pentadbir Sistem ICT, ICTSO

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 11 **HUBUNGAN PEMBEKAL**	
1101 Keselamatan Maklumat Dalam Hubungan Pembekal	
Objektif: Memastikan aset ICT EAIC yang boleh dicapai oleh pembekal dilindungi.	
110101 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal	
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset EAIC. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: i. Mengenal pasti dan didokumentasi 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 kontigasi *(contingency plan)* bagi memastikan ketersediaan kemudahan pemprosesan maklumat; vii. Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber EAIC kepada pembekal; viii. Menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber EAIC (Lampiran B);** dan ix. Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.	STM, Pasukan Projek/Pemilik Projek dan Pembekal

110102 Menangani Keselamatan Dalam Perjanjian 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. Pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak EAIC selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: i. EAIC hendaklah memilih pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; ii. Pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; iii. Semua wakil pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; iv. Produk atau perkhidmatan yang ditawarkan oleh pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;	Pembekal, EAIC

v. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh pembekal; vi. Laporan penilaian pihak ketiga yang dikemukakan oleh 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 EAIC; dan viii. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh EAIC	
110103 Rantaian Bekalan Teknologi Maklumat dan Komunikasi	
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:	Pembekal, EAIC

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.	
1102 Pengurusan Penyampaian Perkhidmatan Pembekal	
Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang diperstujui selaras dengan perjanjian pembekal	
110201 Memantau dan Mengkaji Semula Perkhidmatan Pembekal	
EAIC hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti 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 mengenal insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	Pemilik Projek/Pasukan Projek

110202 Menguruskan Perubahan Kepada Perkhidmatan Pembekal	
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 pembekal; ii. Perubahan yang dilakukan oleh EAIC 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.	STM/Pasukan Projek

BIDANG 12 **PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT**	
1201 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan	
Objektif: Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan.	
120101 Tanggungjawab dan Prosedur	
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden EAIC adalah berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT EAIC yang sedang berkuatkuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: i. Memberikan kesedaran berkaitan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT EAIC dan hebahan kepada warga EAIC sekiranya ada perubahan; dan ii. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.	ICTSO, CSIRT EAIC

120102 Pelaporan Kejadian Keselamatan Maklumat	
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan melalui saluran yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT EAIC. CSIRT EAIC 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 atau 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, atau disyaki hilang; v. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan vi. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan siber berdasarkan: - Pekeliling Am Bilangan 4 Tahun 2022: Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam	ICTSO, dan CSIRT EAIC

120103 Pelaporan Kelemahan Keselamatan Maklumat	
Warga EAIC dan pembekal yang menggunakan sistem dan perkhidmatan maklumat EAIC dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.	Pengguna
120104 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat	
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO
120105 Tindak Balas Terhadap Insiden Keselamatan Maklumat	
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 CSIRT EAIC.** 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;	ICTSO, CSIRT EAIC

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.	
120106 Pembelajaran Daripada Insiden Keselamatan Maklumat	
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.	ICTSO, CSIRT EAIC
120107 Pengumpulan Bahan Bukti	
EAIC hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	ICTSO, CSIRT EAIC

BIDANG 13 **ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN**	
1301 Kesinambungan Keselamatan Maklumat	
Objektif: Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan bisnes EAIC.	
130101 Perancangan Kesinambungan Keselamatan Maklumat	
EAIC hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, EAIC perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi EAIC. EAIC juga perlu mengambil kira keperluan dan ekspetasi 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) EAIC; ii. Menetapkan polisi PKP; iii. Mengenal pasti perkhidmatan kritikal;	Koordinator PKP, Pasukan ERT, CIO, ICTSO, CSIRT EAIC
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 EAIC; vii. Melaksanakan simulasi ke atas dokumen di para (c); dan viii. Melaksanakan penyelenggaran ke atas pelan di para (c).	
130102 Pelaksanaan Kesinambungan Keselamatan Maklumat	
EAIC 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: (j) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal EAIC yang telah dikenal pasti berdasarkan 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) Mengemaskini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal EAIC; (iv) Mengemaskini struktur tadbir urus PKP EAIC jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan (v) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.	Koordinator PKP, Pasukan ERT, CIO, ICTSO, CSIRT EAIC
130103 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat	

EAIC hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.	Setiausaha, Pengarah Bahagian, Koordinator PKP, Pasukan Pasukan ERT, Pemilik Perkhidmatan, Warga EAIC
1302 Lewahan	
Objektif: Untuk memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan**.**	
130201 Ketersediaan Kemudahan Pemprosesan Maklumat	
Kemudahan pemprosesan maklumat EAIC perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (*failover test*) keberkesanannya dari semasa ke semasa.	Pemilik Perkhidmatan dan Pentadbir Sistem ICT

BIDANG 14 **PEMATUHAN**	
1401 Pematuhan Terhadap Keperluan Perundangan dan Kontrak	
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.	
140101 Pengenalpastian Keperluan Undang – Undang dan Kontrak Yang Terpakai	
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga EAIC. Berikut adalah keperluan perundangan perundangan atau peraturan – peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di EAIC dan pembekal di Lampiran A.	Pengguna
140102 Hak Harta Intelek	
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.	Pengguna
140103 Perlindungan Rekod	
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti	Pengguna

yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	
140104 Privasi dan Perlindungan Maklumat Peribadi	
EAIC hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang – undang dan peraturan – peraturan Kerajaan Malaysia.	Pengguna
1402 Kajian Semula Keselamatan Maklumat	
Objektif: Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur EAIC.	
140201 Kajian Semula Keselamatan maklumat Secara Berkecuali	
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pemilik Perkhidmatan/STM
140202 Pematuhan Polisi dan Standard Keselamatan	
EAIC 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.	Pengarah Bahagian dan Pemilik Perkhidmatan
Pelanggaran Polisi Keselamatan Siber EAIC boleh dikenakan tindakan undang-undang dan/atau tatatertib.	Pengguna

LAMPIRAN A

UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Polisi Keselamatan Siber EAIC hendaklah dibaca bersama dengan akta – akta, warta, pekeliling – pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuatkuasa antaranya seperti berikut:

1. Akta 700;
2. Akta Komunikasi dan Multimedia 1998;
3. Akta Tandatangan Digital 1997;
4. Akta Jenayah Komputer 1997;
5. Akta Hak Cipta (Pindaan) Tahun 1997;
6. Akta Rahsia Rasmi 1972;
7. Pekeliling Am Bilangan 4 Tahun 2022: Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam;
8. Pekeliling Perkhidmatan Bil 5 2007 bertajuk “Panduan Pengurusan Pejabat bertarikh 30 April 2007”;
9. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi – Agensi Kerajaan”;
10. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
11. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk “Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam”;
12. Surat Pekeliling Perbendaharaan Bil. 3/1995 – “Peraturan Perolehan Perkhidmatan Perundingan”;
13. Surat Pekeliling Perbendaharaan Bil. 2/1995 (Tambahan Pertama) – “tatacara Penyediaan, Penilaian dan Penerimaan Tender”;

14. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk “Penggunaan Media Jaringan Sosial di Sektor Awam”;
15. 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);
16. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;
17. Arahan Keselamatan;
18. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS);
19. Perintah – Perintah Am;
20. Arahan Perbendaharaan;
21. Arahan Teknologi Maklumat 2007;
22. Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam;
23. Garis Panduan GPKI;

LAMPIRAN B

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER EAIC

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa: -

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

Tarikh: .....