SURUHANJAYA INTEGRITI AGENSI PENGUATKUASAAN
ENFORCEMENT AGENCY INTEGRITY COMMISSION

2026

POLISI KESELAMATAN SIBER

SURUHANJAYA INTEGRITI AGENSI PENGUATKUASAAN

Versi 2.0

SEJARAH DOKUMEN

VERSI	KELULUSAN	TARIKH KUAT KUASA
1.0	Mesyuarat Jawatankuasa Keselamatan ICT Bil 1/2022	27 Oktober 2022
2.0	Mesyuarat Jawatankuasa Keselamatan ICT Bil 1/2025	17 Disember 2025

ISI KANDUNGAN

BAHAGIAN 1

1. PENGENALAN
2. OBJEKTIF
3. KOMPONEN RANGKA KERJA
4. SKOP POLISI
5. PRINSIP

PENGENALAN

Polisi Keselamatan Siber (PKS) 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.

Polisi ini menggariskan standard keselamatan siber untuk EAIC dengan mengaplikasikan prinsip-prinsip daripada *National Cyber Security Baseline* yang dikeluarkan oleh Agensi Keselamatan Siber Negara.

OBJEKTIF

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 utama PKS EAIC 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.

KOMPONEN RANGKA KERJA

Polisi ini digubal merangkumi enam (6) komponen berikut:

i) Tatakelola – mengenal pasti dan mengaplikasikan peranan, dasar dan tatakelola keselamatan siber

ii) Kenal pasti – menyediakan dan menilai aset, risiko dan keupayaan keselamatan siber

iii) Perlindungan – langkah untuk melindungi maklumat dan sistem serta menguatkuasakan prinsip keistimewaan minimum

iv) Pemantauan – mengenal pasti ancaman dan anomali berpotensi serta menjalankan semakan akses secara berkala

v) Tindak Balas – menjalankan tindak balas insiden

vi) Pemulihan – strategik memulihkan operasi dan data selepas insiden

SKOP POLISI

Komponen Skop	Huraian Ringkas
Aset yang Dilindungi	Meliputi **SEMUA** data, perkakasan (PC, komputer riba, peranti mudah alih), perisian, dan kemudahan rangkaian/fizikal yang dimiliki atau digunakan oleh organisasi
Pihak yang Terlibat	Terpakai kepada **SEMUA** kakitangan (termasuk pengurusan atasan) dan pihak ketiga (kontraktor/vendor) yang mempunyai akses kepada aset ICT
Tujuan Teras	Memastikan **Kerahsiaan, Integriti, dan Ketersediaan** (CIANA) maklumat dan sistem kritikal.
Kawalan Utama	Menetapkan peraturan untuk pengurusan risiko, tindak balas insiden, pengurusan capaian (kata laluan/hak akses), dan penggunaan peranti/internet.

PRINSIP-PRINSIP POLISI

1. **Akses Atas Dasar Perlu Mengetahui**

   Akses terhadap penggunaan aset ICT dan sistem hanya diberikan kepada pengguna mengikut peranan pelaksanaan tugasnya sahaja.

2. **Hak Akses Minimum**

   Hak akses kepada pengguna hanya diberi berdasarkan keperluan dan pada tahap set yang paling minimum iaitu untuk membaca dan / atau melihat bagi tujuan pelaksanaan tugas.

3. **Akauntabiliti**

   Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT yang merangkumi data dan sistem maklumat.

4. **Pengasingan Tugas**

   Memastikan tiada individu tunggal mempunyai kawalan ke atas semua aspek dalam tugas atau proses kritikal.

5. **Pengauditan**

   Tujuan aktiviti ini ialah untuk mengenalpasti insiden berkaitan keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT.

6. **Pematuhan**

   PKS 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.

8. **Saling Bergantungan**

BAHAGIAN 2

BIDANG

1. PEMBANGUNAN DAN PENYELENGGARAAN POLISI
2. ORGANISASI KESELAMATAN SIBER
3. KESELAMATAN SUMBER MANUSIA
4. PENGURUSAN ASET ICT
5. KAWALAN AKSES
6. KESELAMATAN FIZIKAL DAN PERSEKITARAN
7. PENGURUSAN OPERASI & KOMUNIKASI
8. PEROLEHAN, PEMBANGUNAN & PENYELENGGARAAN SISTEM
9. PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN MAKLUMAT
10. PENGURUSAN KESINAMBUNGAN PERKHIDMATAN
11. PENGURUSAN RISIKO
12. LATIHAN DAN PROGRAM KESEDARAN
13. AUDIT KESELAMATAN SIBER
14. PEMATUHAN

BIDANG 1: PEMBANGUNAN DAN PENYELENGGARAAN POLISI	
0101 Polisi Keselamatan Siber	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan siber selaras dengan keperluan EAIC dan perundangan yang berkaitan.	
010101 Pembangunan Polisi	**Tindakan**
Pelaksanaan polisi ini akan dijalankan oleh Setiausaha (SU) EAIC selaku Pengerusi Jawatankuasa Keselamatan ICT (JKICT) EAIC dengan dibantu oleh Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Pegawai Teknologi Maklumat, Pentadbir Sistem ICT dan semua Pengarah Bahagian/Unit di EAIC.	STM
010102 Penyebaran Polisi	**Tindakan**
Polisi ini perlu disebarkan kepada semua pengguna data dan sistem maklumat EAIC termasuk pegawai dan kakitangan EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC.	ICTSO
010103 Penyelenggaraan Polisi	**Tindakan**
Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan dan polisi Kerajaan seperti berikut: a) Semakan berkala: ICTSO menyemak polisi secara berkala atau selepas berlaku insiden yang signifikan atau perubahan dalam aspek keselamatan siber; b) Pindaan: Polisi yang dikemas kini akan dibentang kepada pihak berkepentingan; dan c) Dibaca bersama dengan arahan/pekeliling/garis panduan/prosedur yang dikeluarkan oleh Kerajaan dari semasa ke semasa.	ICTSO
010104 Pengecualian Polisi	**Tindakan**
PKS EAIC hendaklah dipatuhi oleh semua pengguna ICT di EAIC dan tiada pengecualian diberikan.	Pengguna

BIDANG 2: ORGANISASI KESELAMATAN SIBER	
0201 Tatakelola	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber EAIC.	
020101 Peranan dan Tanggungjawab JKICT	
(i) Setiausaha EAIC	**Tindakan**
Setiausaha EAIC adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: (a) Menetapkan hala tuju strategik pengurusan keselamatan siber EAIC; (b) Memastikan penguatkuasaan pelaksanaan Polisi ini; (c) Memastikan warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC memahami dan mematuhi peruntukan – peruntukan di bawah Polisi ini; (d) Memastikan sumber dan keperluan yang diperlukan EAIC bagi menjamin keselamatan siber adalah mencukupi; (e) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan (f) Melantik CDO dan ICTSO.	Setiausaha EAIC
(ii) Ketua Pegawai Digital (CDO)	**Tindakan**
Ketua Pegawai Digital (CDO) bagi EAIC ialah Pengarah Bahagian Khidmat Pengurusan (BKP). Peranan dan tanggungjawab CDO adalah seperti berikut: (a) Membantu Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam Polisi ini; (b) Mengesah dan menentukan langkah-langkah keselamatan siber di EAIC;	CDO

(c) Mengesah dan menentukan sama ada insiden siber yang berlaku perlu dilaporkan kepada pihak yang berautoriti seperti Agensi Keselamatan Siber Negara (NACSA) dan Jabatan Suruhanjaya Komunikasi dan Multimedia (SKMM) (d) Memastikan kawalan keselamatan maklumat dalam EAIC diseragam dan diselaraskan dengan sebaiknya; Pengarah BKP juga berperanan sebagai Pengarah *Computer Security Incident Response Team* (CSIRT) EAIC.	
(iii) Pengarah Bahagian	**Tindakan**
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; (d) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa di bahagian.	Pengarah Bahagian
(v) Pengurus ICT	
Pegawai Teknologi Maklumat di STM EAIC adalah merupakan Pengurus ICT. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Mengkaji dan menetapkan kawalan keselamatan siber agar ianya berselaras dengan keperluan jabatan;	

b. Menentukan kawalan capaian semua pengguna terhadap aset ICT EAIC.	
(iv) Pegawai Keselamatan ICT (ICTSO)	
Pegawai Teknologi Maklumat di STM EAIC merupakan Pegawai Keselamatan ICT (ICTSO) dan juga Pengurus (CSIR)EAIC. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Melaksana dan memantau pematuhan Polisi ini kepada Warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC; (b) Mengurus program dan latihan keselamatan siber di EAIC; (c) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya dan khidmat nasihat berkaitan langkah-langkah perlindungan yang bersesuaian; (d) Melaporkan insiden keselamatan siber kepada CDO bagi insiden yang memerlukan Pemulihan Bencana; (e) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; (f) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber.	ICTSO
(v) Pentadbir Sistem ICT	**Tindakan**
Pegawai dan kakitangan Seksyen Teknologi Maklumat EAIC merupakan Pentadbir Sistem ICT. Pentadbir Sistem ICT EAIC adalah terdiri daripada: (a) Pentadbir Rangkaian (b) Pentadbir Sistem Aplikasi/ Portal (c) Pentadbir E-mel	
a) Pentadbir Rangkaian	**Tindakan**

Juruteknik Komputer di STM EAIC merupakan Pentadbir Rangkaian. Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti yang berikut: (a) Memastikan kemudahan rangkaian beroperasi sepanjang masa; (b) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;	Pentadbir Rangkaian
b) Pentadbir Sistem Aplikasi/ Portal	**Tindakan**
Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat di STM EAIC merupakan Pentadbir Sistem Aplikasi/ Portal. Peranan dan tanggungjawab Pentadbir Sistem Aplikasi/ Portal adalah seperti yang berikut: (a) Melaksanakan pemantauan dan penyelenggaraan terhadap portal, sistem aplikasi dalaman EAIC dan aplikasi Kerajaan Digital yang digunakan di EAIC dari semasa ke semasa; (b) Memastikan reka bentuk sistem aplikasi/portal dibangunkan dengan ciri-ciri keselamatan terbina; (c) Memastikan sistem aplikasi/portal mempunyai kawalan capaian yang selamat; (d) Memastikan kelancaran operasi sistem aplikasi/portal supaya perkhidmatan yang disediakan tidak terjejas; (e) Melaporkan sebarang pelanggaran keselamatan sistem aplikasi/portal kepada ICTSO; (f) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; (g) Menganalisis dan menyimpan rekod jejak audit.	Pentadbir Sistem Aplikasi/ Portal
c) Pentadbir E-mel	**Tindakan**

Pegawai dan kakitangan Seksyen Teknologi Maklumat EAIC merupakan Pentadbir E-mel. Peranan dan tanggungjawab Pentadbir E-mel adalah seperti yang berikut: (a) Bertindak sebagai Pentadbir UC di Portal MyGovUC; (b) Melaksanakan proses pengurusan akaun e-mel mengikut prosedur MyGovUC oleh JDN; (c) Memastikan kemudahan capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi; dan (d) Melaporkan sebarang pelanggaran keselamatan e-mel kepada ICTSO.	Pentadbir E-mel
(vi) *Cyber Security Incident Response Team (CSIRT)* EAIC	**Tindakan**
CSIRT EAIC terdiri daripada pegawai dan kakitangan Seksyen Teknologi Maklumat (STM) EAIC yang bertanggungjawab dalam urusan pengendalian insiden keselamatan siber di EAIC selaras dengan Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Keselamatan Siber Sektor Awam dan Arahan Ketua Eksekutif NACSA No. 1 – Pemberitahuan Insiden Keselamatan Siber. Peranan dan tanggungjawab CSIRT EAIC adalah seperti yang berikut: (a) Bertindak sebagai *first-level* support kepada NACSA dalam mengendalikan insiden keselamatan siber di EAIC; (b) Bertanggungjawab dalam pengurusan insiden keselamatan siber yang berlaku di EAIC yang melibatkan: i. Penerimaan dan pengesanan aduan keselamatan siber; ii. Siasatan awal dan tindakan baik pulih;	CSIRT EAIC

(c) Melaporkan dan memohon khidmat nasihat daripada CSIRT JPM dan NACSA berkaitan insiden keselamatan siber di EAIC;	
(vii) Pengguna	**Tindakan**
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. Melaksanakan peraturan berkaitan maklumat terperingkat; iii. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT EAIC dengan segera; iv. Tidak menggunakan pengkomputeran awan bagi tujuan rahsia rasmi iaitu maklumat terperingkat Kerajaan kecuali bagi pengkomputeran awan yang dibangunkan dan dibenarkan oleh pihak Kerajaan; (f) Menghadiri program – program kesedaran mengenai keselamatan siber; dan (g) Mengawal aktiviti penggunaan media sosial seperti berikut: i. Tidak memberi atau mendedahkan sebarang komen atau pernyataan yang menyentuh perkara-perkaa yang boleh menjejaskan imej dan dasar Kerajaan;	Pengguna

ii. Tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan iii. Tidak menggunakan saluran media sosial hingga mengganggu fokus dalam mesyuarat dan urusan kerja. (h) Bersetuju dengan terma dan syarat yang terkandung dalam Polisi ini.	

BIDANG 3: KESELAMATAN SUMBER MANUSIA	
0301 Keselamatan Sumber Manusia Dalam Tugasan Harian	
Objektif: Memastikan semua sumber manusia yang berkaitan merangkumi warga EAIC dan pihak ketiga memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan siber. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.	
030101 Sebelum Perkhidmatan	**Tindakan**
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan EAIC serta pihak ketiga yang terlibat dalam menjamin keselamatan siber sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan, atau, untuk pegawai dan kakitangan EAIC serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan; dan (d) Menandatangani Surat Akuan Pematuhan PKS EAIC seperti di **Lampiran C.**	Pengguna
030102 Dalam Tempoh Perkhidmatan	**Tindakan**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan pegawai dan kakitangan EAIC serta pihak ketiga yang berkepentingan mengurus keselamatan siber berdasarkan perundangan dan peraturan yang ditetapkan oleh EAIC; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan siber diberi kepada pengguna ICT	Pengguna

EAIC secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan EAIC serta pihak ketiga yang berkepentingan dan peraturan ditetapkan oleh EAIC; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan siber. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan, EAIC.	
030103 Penamatan dan Pertukaran Perkhidmatan	**Tindakan**
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; (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; dan (c) Maklumat rasmi EAIC dalam peranti tidak dibenarkan dibawa keluar dari EAIC.	STM dan Warga EAIC
0302 Pihak Ketiga	
Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga seperti pembekal, pakar runding dan lain-lain.	
030201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	**Tindakan**
Pihak ketiga adalah merupakan pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian terhadap aset ICT EAIC.	

Perkara yang perlu dipatuhi termasuk yang berikut: (a) Pihak ketiga hendaklah membaca, memahami dan mematuhi PKS EAIC; (b) Mengenal pasti risiko dan keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (c) Capaian pihak ketiga terhadap aset ICT EAIC perlu berlandaskan kepada keperluan tugas mengikut kontrak yang dipersetujui; (d) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Kawalan dan elemen keselamatan berikut hendaklah diambilkira dalam perjanjian kontrak yang dimeterai: i. Polisi Keselamatan Siber EAIC; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. (e) Menandatangani Surat Akuan Pematuhan PKS EAIC seperti di **Lampiran C**; dan (f) Melengkapkan dan menghantar borang tapisan keselamatan yang berkaitan serta pematuhan melalui Sistem e-Vetting.	CDO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga
030202 Perjanjian Kerahsiaan	**Tindakan**
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan didokumentasikan. Pihak ketiga hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	Pengguna
030203 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	**Tindakan**
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggara oleh pihak ketiga;	

(b)	Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dari semasa ke semasa;	Pengguna
(c)	Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	

BIDANG 4: PENGURUSAN ASET ICT	
0401 Akauntabiliti Aset	
Objektif: Memastikan semua aset ICT EAIC mendapat perlindungan yang bersesuaian yang merangkumi perkakasan, perisian dan data.	
040101 Aset ICT	**Tindakan**
Ini bertujuan memastikan semua aset ICT dikenal pasti, direkod dan diberi kawalan serta perlindungan yang sesuai oleh pemilik aset. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: (a) EAIC hendaklah mengenal pasti Pegawai Penerima Aset 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) Memastikan Pegawai Aset mengesahkan penempatan aset ICT di EAIC; dan (e) Setiap pengguna adalah bertanggungjawab ke atas aset ICT di bawah kawalannya.	Pegawai Penerima Aset, Pegawai Aset, Pembantu Aset dan Warga EAIC
040102 Penggunaan Aset yang Dibenarkan	**Tindakan**
Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	Pegawai Aset, Pembantu Aset dan Warga EAIC

040103 Pemulangan Aset	Tindakan
Warga EAIC hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan, berhenti atau penamatan perkhidmatan atau kontrak.	Warga EAIC
0402 Pengelasan Maklumat	
Objektif: Memastikan data dan maklumat digital diberikan tahap perlindungan yang bersesuaian.	
040201 Pengelasan Maklumat	**Tindakan**
Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.	Pegawai Pengelas
040202 Pengendalian Maklumat	**Tindakan**
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) Memberi 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.	Pengguna

BIDANG 5: KAWALAN AKSES	
0501 Dasar Kawalan Akses	
Objektif: Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.	
050101 Keperluan Kawalan Akses	**Tindakan**
Capaian kepada data dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Kawalan akses ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan akses ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keperluan keselamatan aplikasi; dan (d) Undang-undang dan peraturan berkaitan yang berkuatkuasa semasa;	Pemilik perkhidmatan digital dan Pentadbir Sistem ICT
0502 Kawalan Akses Rangkaian	
Objektif: Menghalang akses tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
050201 Akses Rangkaian	**Tindakan**
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari EAIC. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian EAIC, rangkaian agensi lain dan rangkaian awam;	ICTSO dan Pentadbir Rangkaian/ Pentadbir Sistem ICT

(b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
050202 Kawalan Rangkaian	**Tindakan**
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) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (c) Sebarang penyambungan rangkaian yang bukan di bawah kawalan STM EAIC adalah tidak dibenarkan; (d) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di EAIC sahaja; (e) Kemudahan *wireless* LAN hendaklah dipantau dan dikawal penggunaannya; (f) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; dan (g) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan EAIC.	STM, Pentadbir Sistem ICT/ Pentadbir Rangkaian

050203 Akses Internet	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. ICTSO berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; (b) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh pegawai yang diberi kuasa; (c) Bahan yang dilayari di Internet hendaklah ditentukan ketepatan dan kesahihannya. (d) Pengguna hanya dibenarkan memuat turun bahan yang sah; (e) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; (f) Pengguna adalah dilarang untuk melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap akses internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan bahan, teks ucapan atau lain-lain yang mengandungi unsur lucah.	ICTSO dan Pentadbir Rangkaian/ Pentadbir Sistem ICT
0503 Pengurusan Akses Pengguna	
Objektif: Mengawal akses pengguna ke atas aset ICT EAIC.	
050301 Akaun Pengguna	**Tindakan**
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Perkara – perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh EAIC sahaja boleh digunakan;	Warga EAIC/Pentadbir Sistem ICT/Pentadbir E-mel

(b) Akaun pengguna mestilah unik dan mencerminkan identiti pengguna; (c) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (e) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan EAIC; dan (f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: - Bertukar bidang tugas kerja; - Bertukar bahagian/seksyen/unit; - Bertukar ke agensi lain/tamat tempoh pinjaman; - Bersara; - Berhenti kerja; atau - Ditamatkan perkhidmatan.	
050302 Peruntukan Akses Pengguna	**Tindakan**
Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.	STM
050303 Pengurusan Kata Laluan	**Tindakan**
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) Penggunaan Pengesahan Pelbagai Faktor (MFA) adalah digalakkan bagi sistem yang dibangunkan untuk keselamatan tambahan;	Pengguna

(c) Pertukaran kata laluan hendaklah dilaksanakan jika terdapat bukti dikompromi bagi sistem yang menyokong MFA. Bagi sistem yang tidak menyokong MFA, kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; (d) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (e) 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; (f) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun; (g) Kata laluan paparan kunci *(lock screen)* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (h) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; (i) Kuat kuasakan pertukaran kata laluan semasa atau selepas log masuk kali pertama atau selepas reset kata laluan; (j) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan (k) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
050304 Pembatalan atau Pelarasan Hak Akses	**Tindakan**
Hak akses Warga EAIC dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan / dibatalkan selepas penamatan pekerjaan, kontrak	Pentadbir Sistem ICT

atau perjanjian atau diselaraskan apabila berlaku perubahan dalam EAIC.	
050305 Dasar *Clear Desk* dan *Clear Screen*	**Tindakan**
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuklah seperti yang berikut: (a) Menggunakan kemudahan *sleep mode* dengan kata laluan apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat; dan (d) E-mel masuk dan keluar hendaklah dikawal.	Warga EAIC
0504 Kawalan Akses Aplikasi dan Maklumat	
Objektif: Menghalang akses tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
050401 Akses Aplikasi dan Maklumat	**Tindakan**
Akses kepada sistem aplikasi dan maklumat hendaklah dihadkan mengikut kawalan capaian yang ditetapkan dan bertujuan melindungi daripada sebarang bentuk akses yang tidak dibenarkan.	Pentadbir Sistem ICT/ICTSO

(a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap akses dan keselamatan maklumat yang telah ditentukan; dan (b) Setiap aktiviti akses sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log)	
0505 Kawalan Akses Sistem Pengoperasian	
Objektif: Menghalang akses tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
050501 Akses Sistem Pengoperasian	**Tindakan**
Kawalan terhadap akses sistem pengoperasian perlu mempunyai kaedah pengesahan akses 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; (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.	Pentadbir Sistem/ICTSO
050502 Kawalan Akses Kepada Kod Sumber Program	**Tindakan**
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	Pengarah Projek, Pengurus Projek dan Pentadbir Sistem ICT

(c) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik EAIC.	

0506 Peranti Mudah Alih Dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peranti mudah alih dan kemudahan kerja jarak jauh.	
050601 Peranti Mudah Alih	**Tindakan**
Peranti mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Pengguna
050602 Kerja Jarak Jauh	**Tindakan**
Kerja jarak jauh melibatkan aktiviti mengakses data dan sistem maklumat Suruhanjaya di luar premis oleh warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC. Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi kerja jarak jauh.	Pengguna

BIDANG 6: KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0601 Keselamatan Kawasan	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
060101 Keselamatan Fizikal	**Tindakan**
Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan Aset ICT EAIC. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia. (e) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; (f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan (g) Memasang alat penggera atau kamera keselamatan.	BKP

060102 Kawalan Masuk Fizikal	Tindakan
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
060103 Keselamatan Ruang Kerja dan Kemudahan	**Tindakan**
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Kawasan tempat bekerja, bilik rahsia, bilik fail, bilik kawalan CCTV, bilik siasatan dan bilik rakaman percakapan perlu dihadkan daripada diakses oleh orang luar tanpa kebenaran; (b) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan; dan (c) Akses kepada kawasan larangan hanya kepada pegawai-pegawai yang dibenarkan sahaja.	Pengguna
0602 Keselamatan Perkakasan ICT	
Objektif: Melindungi perkakasan ICT EAIC daripada kehilangan, kerosakan, kecurian dan disalahgunakan.	
060201 Perkakasan ICT	**Tindakan**
Perkakasan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan.	Pengguna

Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut: (a) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan EAIC sahaja. (b) Semua pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; (c) Penggunaan kata laluan untuk akses ke sistem komputer adalah perlu; (d) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (e) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (f) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; (g) 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; (h) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran. (i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; (j) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci;	

(k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (l) Perkakasan ICT guna sama yang hendak dibawa keluar perlulah mendapat kelulusan dan direkodkan bagi tujuan pemantauan; (m) Perkakasan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan kehilangan aset/pelaporan insiden; (n) Pengendalian perkakasan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT; (p) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; (q) 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; (r) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; dan (s) Pengguna dilarang sama sekali mengubah *password Administrator* yang telah ditetapkan oleh pihak ICT.	
060202 Media Storan	**Tindakan**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti fl*ash disk, thumb drive*, pita magnetik, *optical disk* dan media storan lain. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pengguna

(a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Hanya maklumat rasmi dibenarkan untuk disimpan dalam media storan yang dibekalkan oleh EAIC; (e) Semua media storan yang mengandungi maklumat kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (f) Akses dan pergerakan media storan hendaklah direkodkan; (g) Membuat salinan sandaran *(backup copy)* pada media storan yang bersesuaian bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (h) Semua media storan yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan (i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
060203 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan	Pengguna

(c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan.	
060204 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan EAIC; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (c) Lesen perisian *(registration code, serials, CD-keys)* perlu disimpan berasingan daripada CD-rom, disk atau media berkaitan bagi mengelakkan daripada berlakunya kecuaian atau cetak rompak; dan (d) Source code sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Pengguna
060205 Keselamatan Kabel	**Tindakan**
Kabel rangkaian hendaklah dilindungi kerana ia boleh menjadi punca kepada ancaman keselamatan siber sekiranya terdedah dan mudah diakses. Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan dan kerosakan. Langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi; (b) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (c) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;	STM EAIC

(d) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (e) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
060206 Penyelenggaraan Perkakasan ICT	**Tindakan**
Perkakasan ICT hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan perkakasan untuk digunakan. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; (c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan (e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan. (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada STM.	STM, Pentadbir sistem ICT
060207 Keselamatan Perkakasan ICT di Luar Premis	**Tindakan**
Keselamatan perkakasan ICT 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;	Pengguna

ii. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; iii. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan. i. Peralatan ICT yang hendak dibawa keluar dari premis EAIC untuk tujuan rasmi, perlulah mendapat kelulusan pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan ii. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	
060208 Pelupusan Perkakasan	**Tindakan**
Pelupusan melibatkan semua perkakasan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau aset bernilai rendah yang dibekalkan oleh EAIC dan ditempatkan di EAIC. Perkakasan 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, degauzing* atau pembakaran; (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan atau salinan sandaran (*backup copy*); (c) Data dalam perkakasan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan telah dihapuskan dengan cara yang selamat;	Pegawai Aset, Pentadbir Sistem ICT dan warga EAIC

(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 perkakasan ICT; (g) Pelupusan perkakasan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: (a) Menyimpan mana-mana perkakasan ICT yang hendak dilupuskan untuk milik peribadi; (b) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM*, *hardisk*, *motherboard* dan sebagainya; (c) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana perkakasan yang berkaitan ke mana-mana bahagian di EAIC; (d) Memindah keluar dari EAIC mana-mana perkakasan ICT yang hendak dilupuskan; dan (e) Melupuskan sendiri perkakasan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab EAIC. 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 perkakasan komputer yang hendak dilupuskan: (a) 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; (b) Maklumat lanjut berhubung pelupusan boleh dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa; (c) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; (d) Pegawai aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem aset; dan (e) Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dipadam atau ditulis ganti (*overwrite*) dengan betul sebelum dilupuskan atau diguna semula.	
060209 Penggunaan Perkakasan Tanpa Kawalan	**Tindakan**
Pengguna hendaklah memastikan perkakasan yang digunakan tanpa kawalan mempunyai perlindungan sewajarnya: (a) Tamatkan sesi aktif apabila selesai tugas; (b) Log-off komputer meja dan komputer riba apabila sesi bertugas selesai; dan (c) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	Pengguna

BIDANG 7: PENGURUSAN OPERASI & KOMUNIKASI	
0701 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
070101 Pengendalian Prosedur	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua Prosedur Operasi Standard yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pengguna
070102 Pengurusan Perubahan	**Tindakan**
Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau	Pengguna

pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti perubahan komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat.	
0702 Perancangan Sistem dan Pengasingan Tugas	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
070201 Pengurusan Kapasiti	**Tindakan**
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	STM, Pentadbir Sistem ICT
070202 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi	**Tindakan**
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: (a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*).	STM, Pentadbir Sistem ICT

(b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan (c) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.	
070203 Pengasingan Tugas	**Tindakan**
Perkara – perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan; (c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*; dan (d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	ICTSO/ Pengurus ICT
0703 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti *malware* dan sebagainya.	
070301 Kawalan Daripada Perisian Berbahaya	**Tindakan**
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*	STM, Pentadbir Sistem ICT

System (IDS) dan *Intrusion Prevention System (IPS)* di pelayan yang digunakan serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen dan berdaftar; (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) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan *malware*.	
0704 Salinan Sandaran *(Backup)*	
Objektif: Melindungi data agar boleh diakses pada bila-bila masa mengikut ketersediaan data.	
070401 *Backup*	**Tindakan**
Bagi memastikan data dan sistem maklumat dapat diakses semula sekiranya berlaku bencana, *backup* hendaklah dilaksanakan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Membuat *backup* ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi;	STM, Pentadbir Sistem ICT

(c) Menguji sistem *backup* dan *restore* sedia ada bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila perlu digunakan khususnya semasa berlaku kecemasan; 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** (e) Merekod dan menyimpan salinan *backup* di lokasi berlainan dan selamat.	
0705 Pengurusan Media	
Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
070501 Prosedur Pengendalian Media	**Tindakan**
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 dan merekodkan aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua jenis media di tempat yang selamat; dan (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Pengguna

0706 Pengurusan Perkongsian Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara EAIC dan pihak luar terjamin.	
070601 Perkongsian Maklumat	**Tindakan**
Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Polisi, prosedur, dan kawalan perkongsian maklumat dan perisian antara EAIC dan agensi/pihak luar hendaklah diwujudkan untuk melindungi perkongsian data dan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari EAIC; dan (c) Maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	Pengguna
070602 Pengurusan Mel Elektronik (E-mel)	**Tindakan**
Penggunaan e-mel di EAIC perlu mematuhi keperluan etika penggunaan e-mel dan internet yang terkandung dalam Pekeliling Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Akaun e-mel yang diperuntukkan oleh EAIC sahaja yang boleh digunakan. Penggunaan akaun milik orang lain atau dikongsi bersama adalah dilarang; (b) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;	Pengguna

(c) Pengguna hendaklah mengelak membuka e-mel daripada penghantar yang tidak diketahui atau diragui; (d) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; (e) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan serta tidak diperlukan lagi boleh dihapuskan; (f) Mengambil tindakan dengan memberi maklum balas terhadap e-mel dengan segera; (g) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti gmail.com dan sebagainya) tidak boleh digunaan untuk tujuan rasmi; danp (h) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	
0707 Pemantauan *(Monitoring)*	
Objektif: Merekodkan dan menjejak log peristiwa sistem bagi menghasilkan bukti yang diperlukan untuk pemantauan keselamatan.	
070701 Sistem Log	**Tindakan**
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log peristiwa yang merekodkan peristiwa teknikal sistem dan berfungsi sebagai bukti yang didokumenkan yang mempunyai rekod turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Pelaporan kepada ICTSO dan CDO sebelum melaporkan selanjutnya kepada CSIRT EAIC/NACSA adalah perlu, sekiranya wujud aktiviti yang tidak sah seperti kecurian maklumat dan pencerobohan.	Pentadbir Sistem ICT

070702 Jejak Audit	Tindakan
Setiap sistem mestilah mempunyai jejak audit yang merekodkan aktiviti-aktiviti yang berlaku dalam sistem secara kronologi. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti sistem yang tidak mempunyai ciri-ciri keselamatan. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari keosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT
0708 Pengurusan Kerentanan Teknikal *(Vulnerability)*	
Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
070801 Kawalan dari Ancaman Keselamatan Siber	**Tindakan**
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.	Pentadbir Sistem ICT, CSIRT EAIC

Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Memperoleh maklumat teknikal kerentanan yang tepat ke atas sistem maklumat yang digunakan melalui penggunaan perisian pengesanan kerentanan yang sesuai; (b) Menilai tahap kerentanan bagi mengenal pasti tahap risiko yang bakal dihadapi; (c) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; (d) Menganalisis tahap risiko kerentanan; dan (e) Mengambil tindakan pengolahan dan kawalan risiko.	

BIDANG 8: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
0801 Keselamatan dalam Membangunkan Sistem dan Aplikasi	
Objektif: Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan siber yang bersesuaian.	
080101 Keperluan Keselamatan Sistem Maklumat	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna, dan sistem output untuk memastikan data yang diproses adalah tepat; (c) Aplikasi perlu mengandungi semakan pengesahan *(validation)* untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; (d) Semua sistem yang dibangunkan hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; (e) Kod sistem aplikasi yang dibangunkan perlu selari dengan amalan baik pengaturcaraan yang selamat *(secure coding)* berdasarkan garis panduan yang berkuat kuasa, antaranya seperti *OWASP Top 10 (Open Web Application Security Project),* Rangka Kerja Keselamatan Siber Kerajaan	Pentadbir Sistem ICT, ICTSO, Pemilik Sistem

(RAKKSSA) dan Buku Panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA); dan (f) Pengujian keselamatan boleh dilaksanakan bagi memastikan keselamatan sistem maklumat berada pada tahap yang baik.	
080102 Pengesahan Data Input dan Output	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan (b) Data output daripada aplikasi perlu disahkan bagi memastikan keselamatan sistem maklumat berada pada tahap yang baik.	Pentadbir Sistem ICT, ICTSO, Pemilik Sistem
0802 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080201 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: (a) Keselamatan persekitaran pembangunan; (b) Keselamatan pangkalan data; (c) Keperluan keselamatan dalam fasa reka bentuk; (d) Keperluan *check point* keselamatan dalam carta perbatuan projek; (e) Keperluan pengetahuan ke atas keselamatan aplikasi; (f) Keselamatan dalam kawalan versi; dan (g) Bagi pembangunan secara penyumberluaran *(outsource),* pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	ICTSO, STM, Pentadbir Sistem ICT
080202 Prosedur Kawalan Perubahan Sistem	**Tindakan**

Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi 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; c) Pemantauan ke atas penambahbaikan dan pembetulan yang dilakukan oleh pembekal; d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; e) Capaian kepada kod sumber *(source code)* aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja; dan f) Mempunyai keupayaan untuk menamatkan aplikasi secara automatik *(auto logoff)* bagi pengguna tidak aktif *(idle)* selepas suatu tempoh masa yang ditetapkan.	STM, Pentadbir Sistem ICT dan Pemilik Sistem
080203 Persekitaran Pembangunan Selamat	**Tindakan**
Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. EAIC perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: (a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;	STM, Pentadbir Sistem ICT

(b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; (c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; (d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; (e) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan (f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	
080204 Pembangunan Secara *Outsource*	**Tindakan**
EAIC hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource*. 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. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar adalah mengikut amalan terbaik; dan iii. Penerimaan pengujian berdasarkan kepada kualiti dan ketetapan serahan sistem.	STM, Pentadbir Sistem ICT, dan ICTSO
0803 Kawalan Kriptografi	
Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan, keutuhan serta integriti data dan maklumat.	
080301 Enkripsi	**Tindakan**
Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi *(encryption*) bagi menjaga kerahsiaan dan integriti	

data. Tahap perlindungan data menggunakan teknik enkrispi hendaklah dilaksanakan dengan pertimbangan berikut: a) Enkripsi hendaklah digunakan ke atas *data-at-rest* yang dinilai sebagai kritikal berdasarkan penilaian risiko merangkumi elemen kerahsiaan dan integriti; b) Bagi *data-in-transit*, penggunaan talian yang dienkripsi adalah diwajibkan (contoh: penggunaan sijil SSL).	Pemilik Sistem dan Pentadbir Sistem ICT
080302 Tandatangan Digital	**Tindakan**
Penggunaan tandatangan digital ditentukan melalui penilaian risiko yang dilakukan ke atas data dan sistem maklumat. Maklumat terperinci yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. Penggunaan kemudahan tandatangan digital yang disediakan oleh inisiatif kerajaan adalah digalakkan.	Pemilik Sistem dan Pentadbir Sistem ICT
080303 Pengurusan Infrastruktur Kunci Awam (PKI)	**Tindakan**
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pemilik Sistem dan Pentadbir Sistem ICT

BIDANG 9: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN SIBER	
0901 Pengurusan Insiden Keselamatan Siber	
Objektif: Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan siber.	
090101 Mekanisme Pelaporan Insiden Keselamatan Siber	**Tindakan**
Insiden keselamatan siber bermaksud musibah *(adverse event)* yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Insiden keselamatan siber hendaklah dilaporkan kepada ICTSO dan Agensi Keselamatan Siber Negara (NACSA) dalam tempoh yang ditetapkan berdasarkan pekeliling dan arahan yang berkuat kuasa iaitu **Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam** dan **Arahan Ketua Eksekutif NACSA No.1 - Pemberitahuan Insiden Keselamatan.** Perkara yang perlu dipertimbangkan adalah seperti berikut:\ (a) Maklumat didapati atau disyaki hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Prosedur dan Proses Kerja Pelaporan Insiden Keselamatan Siber EAIC adalah seperti di **Lampiran A.**	CSIRT EAIC

090102 Prosedur Pengurusan Maklumat Insiden Keselamatan Siber	**Tindakan**
Maklumat mengenai insiden keselamatan siber yang dikendalikan perlu disimpan dan dianalisis untuk tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Bahan bukti berkaitan insiden keselamatan siber hendaklah disimpan dan diselenggara. Kawalan – kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: (a) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan – pelan pemulihan bencana; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	ICTSO, CSIRT EAIC

BIDANG 10: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
1001 Dasar Kesinambungan Perkhidmatan	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pengguna.	
100101 Pelan Kesinambungan Perkhidmatan (PKP)	**Tindakan**
PKP atau *Business Continuity Plan (BCP)* hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. 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. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Mengenal pasti tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes; (c) Melaksanakan prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang ditetapkan; (d) Mendokumentasi proses dan prosedur yang dipersetujui; (e) Melaksanakan program kesedaran dan latihan kepada pengguna mengenai prosedur kecemasan; (f) Membuat *backup*; dan	CDO, ICTSO, CSIRT EAIC

(g) Menguji dan mengemaskini pelan mengikut keperluan semasa. Pelan PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut keutamaan; (b) Senarai kakitangan EAIC dan pembekal berserta nombor yang boleh dihubungi; (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Salinan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.	

BIDANG 11: PENGURUSAN RISIKO	
1101 Pengurusan Risiko Keselamatan Siber	
Objektif: Menetapkan dan menyelenggara proses untuk mengenal pasti, menilai dan mengurus risiko khusus kepada keselamatan siber.	
110101 Pelan Pengurusan Risiko	**Tindakan**
Penilaian risiko keselamatan siber dilaksanakan dengan merujuk kepada **Surat Pekeliling Am Bil 3 Tahun 2024 – Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam dan Arahan Ketua Eksekutif NACSA No. 5 – Penilaian Risiko Keselamatan Siber** dan pekeliling yang berkuat kuasa.	ICTSO, STM
110102 Proses Pengurusan Risiko	**Tindakan**
Proses berikut akan digunapakai dalam mengurus risiko keselamatan siber: (a) Pengenalpastian risiko: Melakukan penilaian berkala terhadap risiko yang berpotensi, termasuk kelemahan dalaman dan ancaman luaran. (b) Penilaian risiko: Menilai kebarangkalian dan impak risiko yang dikenal pasti. (c) Pengurangan (rawatan) risiko: Membangunkan strategi untuk menangani risiko tinggi, termasuk melaksanakan kawalan tambahan dan menyesuaikan proses.	ICTSO, STM

BIDANG 12: LATIHAN DAN PROGRAM KESEDARAN	
1201 Latihan dan Kesedaran	
Objektif: Merancang dan menetapkan strategi latihan dan kesedaran keselamatan siber yang berterusan kepada semua pegawai dan kakitangan EAIC.	
120101 Sasaran Latihan dan Program Kesedaran	**Tindakan**
Program kesedaran: Menjalankan kempen kesedaran untuk mendidik pegawai dan kakitangan EAIC berkenaan kepentingan keselamatan siber dan peranan dalam melindungi data organisasi. Diberikan kepada pegawai dan kakitangan EAIC berkaitan keselamatan siber yang tidak bersifat teknikal **Latihan khusus:** Menawarkan latihan mendalam kepada pegawai dan kakitangan di jawatan penting (contoh: IT, pengurusan) berkenaan topik keselamatan siber.	ICTSO dan STM

BIDANG 13: AUDIT KESELAMATAN SIBER	
1301 Audit Keselamatan Siber	
Objektif: Menetapkan pelaksanaan audit bagi memastikan pematuhan yang berterusan kepada perundangan, garis panduan dan polisi berkaitan	
130101 Jaminan Keselamatan Siber	**Tindakan**
Bagi memastikan jaminan keselamatan siber, audit boleh dilaksanakan mengikut keperluan melalui kaedah seperti berikut: (a) Audit secara kendiri - Dilaksanakan oleh individu atau pasukan dalam EAIC untuk menilai pematuhan terhadap polisi dan standard keselamatan siber yang ditetapkan, biasanya dilakukan secara berkala. (b) Audit dalaman - Dilaksanakan oleh fungsi audit dalaman agensi untuk memberikan penilaian objektif mengenai keberkesanan kawalan keselamatan siber dan sistem pengurusan risiko (c) Audit pihak ketiga - Audit yang dijalankan oleh firma atau juruaudit luar yang bebas untuk memberikan pandangan yang tidak bias dan pengesahan luaran terhadap tahap keselamatan siber agensi	ICTSO dan STM

BIDANG 14: PEMATUHAN	
1401 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan dan memantapkan tahap keselamatan siber bagi mengelak daripada pelanggaran kepada Polisi Keselamatan Siber EAIC.	
140101 Pematuhan Polisi	**Tindakan**
Setiap pengguna di EAIC hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber EAIC dan undang-undang serta peraturan lain yang berkuat kuasa. ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi polisi, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan siber.	Pengguna
140102 Pelanggaran Polisi	**Tindakan**
Pelanggaran Polisi Keselamatan Siber EAIC boleh dikenakan tindakan undang-undang dan/atau tatatertib atau digantung akses/capaian kepada kemudahan ICT EAIC.	Pengguna

BAHAGIAN 3

1. GLOSARI
2. LAMPIRAN A
3. LAMPIRAN B
4. LAMPIRAN C

GLOSARI

(1) Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita *magnetic, optical disk, flash disk,* CD-ROM untuk sebarang kemungkinan adanya virus
(2) Anomali	Keadaan atau sesuatu yang tidak biasa, luar biasa, atau menyimpang dari norma atau corak yang dijangkakan. Dalam konteks teknikal dan keselamatan maklumat, anomali sering digunakan untuk merujuk kepada tingkah laku atau kejadian yang berbeza daripada kebiasaan, yang mungkin menunjukkan terdapatnya masalah, kecacatan, atau ancaman
(3) Aset ICT	Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya berlaku kehilangan, kerosakan atau perubahan. Dalam konteks keselamatan maklumat, aset boleh dikategorikan kepada beberapa kumpulan antaranya proses kerja, data/maklumat, perisian, perkakasan, perkhidmatan, sumber manusia dan tapak / premis. (Surat Pekeliling Am Bil 3 Tahun 2024)
(4) 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.
(5) *Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
(6) BCP/PKP	*Business Continuity Planning* Pelan Kesinambungan Perkhidmatan
(7) 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.
(8) CDO	*Chief Digital Officer*

	Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi
(9) *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.
(10) CSIRT EAIC	*Cyber Security Incident Response Team (CSIRT)* EAIC atau Pasukan Tindak Balas Insiden Keselamatan Siber EAIC Ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan siber di agensi masing-masing dan agensi di bawah kawalannya.
(11) *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.*
(12) *Data-in-transit* (data dalam pergerakan)	Merujuk kepada aliran data yang melalui mana-mana rangkaian. Ini mewakili data yang sedang dipindahkan.
(13) *Data-in-use* (data dalam penggunaan)	Merujuk kepada data yang tidak sekadar disimpan di suatu tempat, tetapi sedang bergerak atau dipindahkan secara aktif dari satu lokasi ke lokasi yang lain.
(14) *Encryption*	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
(15) ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
(16) ICTSO	ICT *Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.

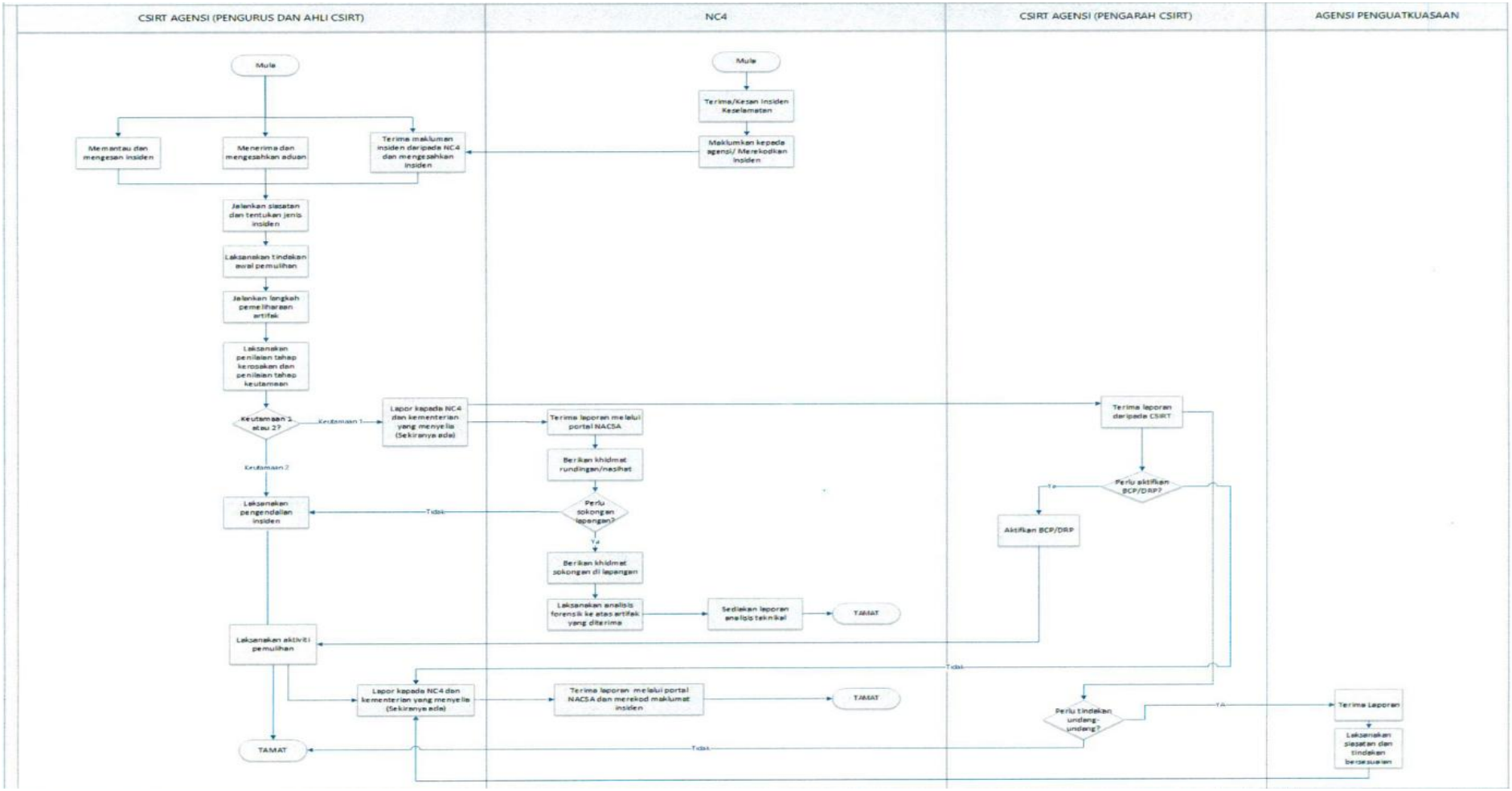
(17) *Internet*	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
(18) *Instrusion Detection System* (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
(19) *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.
(20) JDN	Jabatan Digital Negara
(21) Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
(22) Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data maklumat.
(23) LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer
(24) *Lock*	Mengunci komputer
(25) *Logout*	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
(26) *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.

(27) MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
(28) 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.
(29) NACSA	National Cyber Security Agency Agensi Keselamatan Siber Negara
(30) *Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
(31) Pasukan ERT	Pasukan Tindakan Kecemasan/Emergency Response Team (ERT)
(32) Pasukan Projek	Pasukan yang terdiri daripada satu atau lebih kumpulan yang akan memberi fokus kepada bidang teknikal dan bisnes mengikut keperluan dan kesesuaian projek.
(33) Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
(34) 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.
(35) Pemilik sistem	Individu yang bertanggungjawab terhadap hampir keseluruhan proses kerja projek tersebut. Pemilik sistem memainkan peranan utama menentukan keperluan, spesifikasi dan ciri-ciri serahan (produk atau perkhidmatan) yang akan dihasilkan oleh projek tersebut.

(36) Pengarah Bahagian	Bertanggungjawab melaksanakan hal ehwal pengurusan dan pembangunan organisasi di bahagian
(37) Pengarah BKP (Bahagian Khidmat Pengurusan)	Bertanggungjawab melaksanakan hal ehwal pengurusan dan pentadbiran di BKP EAIC
(38) Pengguna	Merujuk kepada warga EAIC, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT EAIC.
(39) Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksanakan berdasarkan hasil penilaian risiko.
(40) Pengurus ICT	Pegawai yang bertanggungjawab terhadap perancangan dan pengurusan infrastruktur dan pembangunan aplikasi ICT jabatan.
(41) 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.
(42) Pihak Ketiga	Merangkumi pembekal perkhidmatan, pakar runding, kontraktor, vendor, serta pihak luaran lain yang berkaitan
(43) Polisi Keselamatan Siber	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 siber
(44) *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.
(45) 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.
(46) *Server*	Pelayan komputer
(47) SKMM	Suruhanjaya Komunikasi dan Multimedia Malaysia
(48) *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.
(49) Virus	Atur cara yang bertujuan merosakkan data atau aplikasi sistem aplikasi.
(50) Warga EAIC	Kakitangan yang berkhidmat di EAIC sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT EAIC.
(51) *Wireless* LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
(52) *Worm*	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

PROSES KERJA PELAPORAN INSIDEN KESELAMATAN SIBER EAIC



LAMPIRAN B

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 berkuat kuasa antaranya seperti berikut:

1. Akta Suruhanjaya Integriti Agensi Penguatkuasaan (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
8. Pekeliling Am Bilangan 4 Tahun 2022: Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam;
9. Pekeliling Perkhidmatan Bil 5 2007 bertajuk “Panduan Pengurusan Pejabat bertarikh 30 April 2007”;
10. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi – Agensi Kerajaan”;
11. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
12. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk “Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam”;
13. Surat Arahan Ketua Pengarah MAMPU bertarikh 8 April 2011 bertajuk “Penggunaan Media Jaringan Sosial di Sektor Awam”;
14. 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);

15. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;
16. Arahan Keselamatan (Semakan dan Pindaan 2017).;
17. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS);
18. Perintah – Perintah Am;
19. Pekeliling Perbendaharaan~~;~~
20. Arahan Teknologi Maklumat 2007;
21. Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam;
22. Pekeliling Pendigitalan Perkhidmatan Awam Bilangan 4 - Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (Government Public Key Infrastructure – MyGPKI) Tahun 2025
23. Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 – Pematuhan Tatacara Pengguna E-mel dan Internet;
24. Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication* (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa;

LAMPIRAN C

SURUHANJAYA INTEGRITI AGENSI PENGUATKUASAAN
ENFORCEMENT AGENCY INTEGRITY COMMISSION

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: .....