DASAR KESELAMATAN ICT (DKICT) LEMBAGA KEMAJUAN WILAYAH KEDAH (KEDA)

VERSI 3.0

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) di Lembaga Kemajuan Wilayah Kedah (KEDA). Dasar ini juga menerangkan kepada semua pengguna di KEDA mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT. Dasar ini dibuat berasaskan kepada Dasar Keselamatan ICT MAMPU yang sedia ada.

OBJEKTIF

Dasar Keselamatan KEDA diwujudkan untuk menjamin kesinambungan urusan KEDA dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama Keselamatan ICT KEDA ialah seperti berikut:

(a) Memastikan kelancaran operasi KEDA dan meminimumkan kerosakan atau kemusnahan;
(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
(c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

PENYATAAN DASAR

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

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

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

Dasar Keselamatan ICT KEDA merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
(b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
(c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
(d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan
(e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Aset ICT KEDA terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT KEDA menetapkan keperluan-keperluan asas berikut:

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

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

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

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KEDA. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

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

(c) Perkhidmatan

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

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

(d) Data atau Maklumat

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

(e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian KEDA bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

(f) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (e) di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT KEDA dan perlu dipatuhi adalah seperti berikut:

a. Akses atas dasar perlu mengetahui

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

b. Hak akses minimum

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

c. Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah 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.

d. Pengasingan

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

e. Pengauditan

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

f. Pematuhan

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

g. Pemulihan

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

h. Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

KEDA hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu KEDA perlu mengambil langkah-langkah pro-aktif 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.

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

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

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

(b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;

(c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

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

BIDANG 01

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT

Objektif :

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

010101 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh Pengerusi JPICT KEDA dan dan dibantu oleh: i. Ketua Pegawai Maklumat (CIO) ii. Pengurus ICT	Pengerusi JPICT KEDA
010102 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna di KEDA (termasuk kakitangan, pelajar, pembekal, pakar runding, komuniti dan lain-lain.)	ICTSO
010103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT KEDA: (a) Kenal pasti dan tentukan perubahan yang diperlukan; Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat JPICT KEDA; (b) Perubahan yang telah dipersetujui oleh JPICT KEDA dimaklumkan kepada semua pengguna; dan	ICTSO

(c) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun (apabila perlu).	
010104 Pengecualian Dasar	
Dasar Keselamatan ICT KEDA adalah terpakai kepada semua pengguna ICT KEDA dan tiada pengecualian Pengguna diberikan.	Semua

BIDANG 02

ORGANISASI KESELAMATAN

0201 Infrastruktur Keselamatan Organisasi

Objektif :
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT KEDA.

020101 Ketua Pengarah

Peranan dan tanggungjawab Pengurus Besar KEDA adalah seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT KEDA; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT KEDA; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT KEDA; (e) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT KEDA.	Pengurus Besar KEDA

020102 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) adalah Timbalan Ketua Pengarah (Strategik) di KEDA. Peranan dan tanggungjawab beliau adalah seperti berikut:	CIO

(b) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (c) Menentukan keperluan keselamatan ICT; dan (d) Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT. (e) Bertanggungjawab ke atas perkara-perkara yang berkaitan keselamatan ICT KEDA	CIO
020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) adalah pegawai yang dilantik oleh KEDA. Peranan dan tanggungjawab beliau adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT KEDA; (b) Menguatkuasakan Dasar Keselamatan ICT KEDA; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT KEDA kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT KEDA; (e) Menjalankan pengurusan risiko; (f) Menjalankan audit, mengkaji semula, merumus tindak balas Pengurus Besar KEDA berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (CERT) KEDA dan memaklumkannya kepada CIO; (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;	ICTSO

(j) Menyiasat dan mengenalpasti pengguna yang melanggar dasar keselamatan ICT KEDA. (k) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
020104 Ketua Unit Teknologi Maklumat	
Ketua Unit Teknologi Maklumat adalah pegawai yang bertanggungjawab dalam unit ICT di KEDA. Peranan dan tanggungjawab Ketua Unit Teknologi Maklumat adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KEDA; (b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KEDA; (c) Menentukan kawalan akses semua pengguna terhadap aset ICT KEDA; (d) Melaporkan penemuan mengenai pelanggaran Dasar Keselamatan ICT kepada ICTSO; dan (e) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KEDA.	Ketua Unit Teknologi Maklumat
020105 Pentadbir Sistem ICT	
Pentadbir Sistem ICT adalah pegawai yang dilantik bertanggungjawab dalam mentadbir sistem ICT di KEDA. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; (b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT KEDA; (c) Memantau aktiviti capaian harian pengguna;	Pentadbir Sistem ICT

(d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (e) Menyimpan dan menganalisis rekod jejak audit; (f) Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; dan (g) Memastikan pembangunan sistem aplikasi mengambil kira dan mematuhi ciri-ciri keselamatan yang termaktub di dalam Dasar Keselamatan ICT KEDA.	
020106 Pegawai Aset ICT	
(a) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik. (b) Memastikan aset ICT milik KEDA dilabel dan direkodkan. (c) Memastikan aset ICT untuk pinjaman dan simpanan sebelum agihan diletakkan di dalam bilik yang mempunyai kawalan keselamatan terjamin. (d) Memastikan aset ICT yang ingin dilupuskan dilaksanakan mengikut garis panduan kawalan keselamatan bagi pelupusan data digital.	Pegawai Aset ICT
020107 Pengguna	
Pengguna adalah pihak yang menggunakan perkhidmatan dan aset ICT KEDA. Peranan dan tanggungjawab pengguna adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KEDA; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;	Semua

(d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsian maklumat KEDA. (e) Melaksanakan langkah-langkah perlindungan seperti 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 untuk digunakan; (iv) Menjaga kerahsiaan kata laluan; (v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO, Pengurus ICT atau Pentadbir Sistem ICT dengan segera; (g) Menghadiri program-program kesedaran mengenai keselamatan ICT; (h) Bertanggungjawab ke atas aset-aset ICT dbawah jagaannya; dan (i) Menandatangani surat akuan pematuhan Dasar Keselamatan ICT KEDA.	Semua
020108 Jawatankuasa Pemandu ICT KEDA	
Jawatankuasa Pemandu ICT KEDA adalah bertanggungjawab dalam menentukan halatuju ICT dan keselamatan ICT KEDA. Pengerusi : CIO Ahli : (1) ICTSO (2) Pengurus Bahagian / Ketua Unit / KEDA (3) Pegawai yang mempunyai kepakaran di dalam bidang ICT Urus Setia : Unit Teknlogi Maklumat KEDA	Jawatankuasa Pemandu ICT KEDA

Bidang kuasa: (a) Memperakukan/meluluskan dokumen DKICT KEDA; (b) Memantau tahap pematuhan keselamatan ICT; (c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam KEDA yang mematuhi keperluan KEDA; (d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (e) Memastikan KEDA selaras dengan dasar-dasar ICT kerajaan semasa; (f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (g) Membincang tindakan yang melibatkan pelanggaran KEDA; dan; (h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	Jawatankuasa Pemandu ICT KEDA
020109 Pasukan Tindak Balas Insiden Keselamatan ICT KEDA	
Keanggotaan CERT adalah seperti berikut: Pengurus : ICTSO Ahli : (1) Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat KEDA yang dilantik; Peranan dan tanggungjawab CERT adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b. Merekod dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas (response) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum. d. Menasihati KEDA dalam mengambil tindakan pemulihan dan pengukuhan;	CERT

e. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT.	CERT
0202 Pihak Ketiga	
Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, pakar runding dan lain-lain).	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut : (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KEDA; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (d) Akses kepada aset ICT KEDA perlu berlandaskan kepada perjanjian kontrak; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. (i) Dasar Keselamatan ICT KEDA; (ii) Tapisan Keselamatan (iii) Perakuan Akta Rahsia Rasmi 1972; dan (iv) Hak Harta Intelek. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT KEDA sebagaimana Lampiran 1.	Pembekal, Pakar Runding dan Lain-lain

BIDANG 03

KAWALAN ASET DAN PENGKELASAN MAKLUMAT

0301 Akauntabiliti Aset

Objektif :

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KEDA.

030101 Inventori Aset

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

0302 Pengelasan dan Pengendalian Maklumat

Objektif :

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

030201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen. Arahan Keselamatan seperti berikut: (a) rahsia besar; (b) rahsia; (c) sulit; atau (d) terhad	Semua
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

BIDANG 04

KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif :

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

040101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan KEDA serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan KEDA serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

040102 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan pegawai dan kakitangan KEDA serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT	

berdasarkan perundangan dan peraturan yang ditetapkan oleh KEDA; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT KEDA 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 KEDA serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh KEDA; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada KEDA.	Semua
040103 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada KEDA 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 oleh KEDA dan/atau terma perkhidmatan.	Semua

BIDANG 05

KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

Objektif :

Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

050101 Kawalan Kawasan

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

(j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102 Kawalan Masuk Fizikal	
(a) Setiap kakitangan di KEDA hendaklah memakai atau mengenakan kad ID agensi sepanjang waktu bertugas; (b) Semua kad ID agensi hendaklah diserahkan balik kepada KEDA apabila pengguna berhenti atau bersara; (c) Setiap pelawat perlu mendaftar dan mendapatkan Pas Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; (d) Kehilangan pas pelawat mestilah dilaporkan dengan segera kepada Bahagian Khidmat Perunding, KEDA; (e) Hanya kakitangan dan pelawat yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT tertentu KEDA.	Semua dan pelawat
050103 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di KEDA adalah bilik Pengurus Besar, Timbalan Pengurus Besar, bilik server dan lain-lain kawasan yang diwartakan sebagai kawasan larangan. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai- pegawai yang diberi kuasa sahaja : (a) Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu.	Semua dan pelawat

(b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan (c) Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Pengurus Besar KEDA.	Semua dan pelawat
050201 Peralatan ICT	
Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pegawai Aset ICT; (e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) 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; (g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;	Semua

(i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply*(UPS); (j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-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) Peralatan ICT yang hendak dibawa keluar dari premis KEDA, perlulah mendapat kebenaran bertulis dari Pegawai Aset ICT dan direkodkan seperti yang dinyatakan dalam Pekeliling Perbendaharaan sedia ada bagi tujuan pemantauan; (m) Peralatan ICT yang hilang hendaklah dilaporkan mengikut Pekeliling Perbendaharaan sedia ada. (n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (o) Pengguna tidak dibenarkan mengubah lokasi komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset ICT; (p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pegawai Aset ICT untuk di baik pulih; (q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pegawai Aset ICT; (t) Pengguna bertanggunagjawab terhadap perkakasan, perisisan dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (u) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF” apabila meninggalkan pejabat; (v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan	Semua

(w) Memastikan plag dicabut daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	Semua
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat : (a) Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (e) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; (f) Pergerakkan media storan hendaklah direkodkan; (g) Perkakasan backup hendaklah diletakkan ditempat yang terkawal; (h) Mengadakan Salinan atau penduaan (backup) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (i) Semua media storan data yang hendal dilupuskan mestilah dihapuskan dengan teratur dan selamat.	Semua

050203 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan KEDA; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran ketua Unit Teknologi Maklumat; (c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
050204 Penyelenggaraan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. (a) Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; (b) Perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap pperkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habus tempoh jaminan; (d) Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan (e) Semua penyelenggaraan mestilah mendapat kebenaran daripada Ketua Unit ICT; (f) Semua aktiviti penyelengaaran perlu direkodkan. (g) Maklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan;	

050205 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat	
Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan : (a) Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan Pengurus Besar KEDA dan tertakluk kepada tujuan yang dibenarkan; dan (Rujuk Pekeliling Perbendaharaan Bil 5. Tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan) (b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Semua
050206 Peralatan di Luar Premis	
Bagi perkakasan yang dibawa keluar dari premis KEDA, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan KEDA: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
050207 Pelupusan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KEDA dan ditempatkan di KEDA. Peralatan ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KEDA: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding*, *degauzing* atau pembakaran;	Semua

(b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; (c) Peralatan ICT akan dilupuskan hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh 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) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; (g) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: (i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. (ii) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM, hardisk, motherboard* dan sebagainya; (iii) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di KEDA; (iv) Memindah keluar dari KEDA mana-mana peralatan ICT yang hendak dilupuskan; (h) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggungjawab Pegawai Aset KEDA; (i) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti thumb drive, external hard disk sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	Semua

0503 Keselamatan Persekitaran	
Objektif : Melindungi aset ICT KEDA dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pegawai Keselamatan Jabatan yang dilantik. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil : (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; (c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; (d) Bahan Mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan asset ICT; (e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari asset ICT; (f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran perlatan ICT; dan (g) Semyua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	Semua, Unit ICT dan ICTSO

050302 Bekalan Kuasa	
(a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai. (b) Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	37 dari 80 Unit ICT dan ICTSO
050303 Kabel	
Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan wire tapping; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Unit ICT dan ICTSO

050304 Prosedur Kecemasan	
(a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MAMPU 2004; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik.	Semua dan Pegawai Keselamatan Jabatan
0504 Keselamatan Dokumen	
Objektif : Melindungi maklumat KEDA dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua

BIDANG 06

PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur

Objektif :

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

060101 Pengendalian Prosedur

(a) Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan (c) pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (d) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan. (e) Semua kakitangan KEDA hendaklah mematuhi prosedur yang telah ditetapkan.	Semua

060102 Kawalan Perubahan

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

(b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh Juruteknik Komputer KEDA atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus ICT dan ICTSO

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
0603 Perancangan dan Penerimaan Sistem	
Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti	
(a) 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 (b) 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.	Pentadbir Sistem ICT, ICTSO

060302 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. (d) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; (e) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (f) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Pentadbir Sistem ICT dan ICTSO
0604 Perisian Berbahaya	
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.	
060401 Perlindungan Dari Perisian Berbahaya	
(a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (d) Mengemaskini anti virus dengan *pattern* anti virus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;	Semua

(b) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (c) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (d) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
060402 Perlindungan daripada *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	
0605 Housekeeping	
Objektif : Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
060501 Penduaan (*Backup)*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Perkara – perkara yang perlu dipatuhi adalah seperti berikut :- (a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan penduaan bergantung kepada tahap kritikal maklumat;dan (c) Menguji sistem penduaan dan prosedur *restore* yang sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	Semua

(d) Menyimpan sekurang-kurangnya tiga (3) generasi backup; dan (e) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	
0606 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah di kawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan :- (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan mestilah melalui proses *Factory Acceptance Check (FAC)* semasa pemasangan dan konfigurasi; (e) Firewall hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat terperingkat Kerajaan serta dikonfigurasi sendiri oleh pentadbir sistem; (f) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan KEDA; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;	Unit ICT

(h) Memasang perisian *Intrusion Detection System (IDS)* atau *Intrusion Prevention System (IPS)* bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KEDA; (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang. (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan KEDA hendaklah mendapat kebenaran ICTSO; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian KEDA sahaja. Penggunaan modem adalah dilarang sama sekali; dan; (l) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum. (m) Sebarang penyambungan rangkaian daripada pihak ketiga (*remote tunneling*) ke dalam sistem rangkaian KEDA hendaklah mendapat kebenaran ICTSO; (n) Kemudahan bagi *wireless LAN* perlu dipastikan kawalan keselamatan.	Unit ICT
0607 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada CIO terlebih dahulu.	Semua
060702 Prosedur Pengendalian Media	
(a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja;	Semua

(c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; dan (f) Media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	Semua
060703 Keselamatan Sistem Dokumentasi	
(a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Semua
060704 Tatacara Pengurusan Media Storan	
Pengurusan media storan ialah merupakan garis panduan bagi menguruskan media storan yang mengandungi maklumat sulit dan rahsia rasmi kerajaan. Media storan merangkumi perkakasan seperti *cd, tape*, *thumb drive*, *memory card*, *external hard disk* dan lain-lain pperkakasan yang boleh digunakan untuk menyimpan maklumat elektronik. Bagi menjamin keselamatan maklumat yang disimpan di dalam media storan, pengguna adalah dinasihatkan mengikut garis panduan yang berikut: (a) Setiap bahagian mestilah mempunyai kaedah atau prosedur kawalan inventori dan pelupusan media storan; (b) Setiap media storan juga perlulah dilabelkan (*volume label*) untuk memudahkan pengecaman hak milik. Media storan perlulah dilabelkan mengikut Bahagian/Unit/Nama;	ICTSO, Unit ICT, Semua

(c) Semua akses kepada media storan hendaklah dilog; (d) Pengguna hendaklah memastikan media storan yang dibekalkan hanya untuk kegunaan urusan rasmi KEDA; (e) Media yang mengandungi maklumat atau rahsia rasmi mestilah disimpan dengan selamat dan dilabelkan mengikut pengelasannya sama ada Terhad, Sulit atau Rahsia; (f) Hanya kakitangan yang diberi kuasa oleh ICTSO sahaja yang dibenarkan mengakses media yang mengandungi maklumat rahsia rasmi; (g) Pengguna dilarang menyalin, membawa keluar atau memberi media yang mengandungi maklumat rahsia rasmi kepada orang lain. Ini adalah untuk mengelak dari berlakunya pembocoran rahsia; (h) Pengguna disarankan untuk melakukan kaedah pemantapan (*compress*) untuk mengurangkan saiz fail bagi memaksimumkan penggunaan media storan; (i) Setiap media storan termasuklah media storan luar mestilah sentiasa diimbas sebelum digunakan. Media storan hendaklah dilakukan nyah virus untuk mengelakkan penyebaran virus, cecacing atau program yang ditanam ke dalam sistem rangkaian; (j) Media yang mengandungi maklumat yang tidak diperlukan lagi, perlulah dipadamkan (*delete*) sebelum digunakan untuk tujuan lain; (k) Pengguna hendaklah memastikan keselamatan fizikal terhadap media dari ancaman seperti sinaran matahari, suhu panas, elektrostatik dan magnet serta disimpan di tempat yang selamat. Ini dapat mengelakkan maklumat atau data menjadi rosak (*corrupted*) atau tidak boleh dibaca; (l) Bagi penggunaan *Thumb drive*, ia mestilah dikeluarkan daripada sistem dengan cara yang betul. Pengguna dilarang mengeluarkan *thumb drive* dari USB dengan cara terus; (m) Sekiranya disket yang digunakan adalah telah lama jangka hayatnya, kandungan fail atau maklumat di dalamnya perlulah dipindahkan ke media lain seperti CD, *thumb drive* dan lain-lain media storan;	ICTSO, Unit ICT, Semua

(n) Pengguna tidak digalakkan untuk berkongsi penggunaan media storan bagi mengelakkan maklumat yang disimpan di dalam media storan diakses oleh pengguna yang tidak berhak; (o) Semua media storan yang rosak atau tidak boleh digunakan lagi, perlulah di format untuk semua untuk memadamkan kesemua data di dalamnya sebelum dilupuskan dan dimusnahkan; (p) Pelupusan dilakukan sama ada dengan merincih, menggunting atau dibakar sebelum dibuang; (q) Pengguna juga dikehendaki memulangkan semula media storan kepada pihak pengurusan KEDA sekiranya bertukar atau berpindah; dan (r) Sebarang kehilangan dan ancaman terhadap maklumat yang terkandung di dalam media hendaklah dilaporkan kepada ICTSO atau Pegawai Keselamatan Jabatan.	ICTSO, Unit ICT, Semua
060705 Pengurusan Sanitasi Media	
Definisi : Proses penyingkiran data daripada media storan dengan jaminan, bahawa data tidak boleh diambil dan dicapai semula. Rasional : Tujuan dasar ini adalah untuk mewujudkan satu standard pelupusan bersesuaian untuk media elektronik yang mengandungi data sensitif. Prosedur-prosedur pelupusan yang digunakan akan bergantung kepada jenis kecenderungan media tersebut. Media elektronik mungkin dijadualkan untuk kegunaan semula pembaikan, penggantian atau penyingkiran daripada perkhidmatan kerana beberapa sebab dan dihapuskan dalam pelbagai cara seperti yang diterangkan di bawah. Prosedur : (a) Jika penyingkiran dilakukan dengan menulis ganti data, seluruh media / peranti ini mestilah ditulis ganti dengan sekurang-kuangnya tiga kali format.	ICTSO dan Unit ICT

(b) Peralatan yang boleh menyimpan maklumat terperingkat, seperti *desktop* dan komputer riba atau pemacu keras luaran, perlu dipadam sebelum pelupusan. (c) Satu-satunya kaedah fizikal yang boleh diterima untuk memusnahkan media storan seperti cakera keras ialah dengan mencarik, *pulverizing*, dipecahkan atau pembakaran. (d) *Degaussing* adalah satu kaedah yang boleh digunapakai untuk membersihkan data dari media storan. Sila maklum, kaedah ini akan menyebabkan media tidak boleh digunakan.	ICTSO dan Unit ICT
060706 Prosedur Pengendalian Media Sandaran (*backup*)	
Prosedur Pengendalian media sandaran (*backup*) ialah merupakan garis panduan bagi menguruskan media sandaran (*bakup*) yang mengandungi maklumat sulit dan rahsia rasmi kerajaan. Media sandaran (*backup*) merangkumi perkakasan seperti *external hard disk*, *server* dan lain-lain perkakasan yang boleh digunakan untuk menyimpan maklumat elektronik. Bagi menjamin keselamatan maklumat yang disimpan di dalam media sandaran (*backup*), pengguna adalah dinasihatkan mengikut garis panduan yang berikut: (a) Penyediaan Media Sandaran perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. (b) Penghantaran Media Sadaran Proses penghantaran perlu dilindungi dengan ciri-ciri keselamatan. Setiap proses penghantaran perlu direkod di dalam buku log dan di sahkan oleh ICTSO. (c) Penyimpanan Media Sandaran di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat. Perkakasan backup ini hendaklah diletakkan di tempat yang terkawal. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja.	CIO, ICTSO dan Unit ICT

Sekiranya penyimpanan media sandaran di luar premis (*offsite*), peralatan tersebut perlu dilindungi dan dikawal sepanjang masa. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. (d) Penggunaan dan Pelupusan Media Sandaran Penghapusan maklumat atau kandungan media storan mestilah mendapat kebenaran pemilik maklumat terlebih dahulu dan mendapat kelulusan daripada ICTSO dan CIO	ICTSO, Unit ICT, Semua
0608 Pengurusan Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (e) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (f) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KEDA dengan agensi luar; (g) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KEDA; dan (h) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
060802 Mel Elektronik	
(a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh KEDA sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh KEDA; (c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;	Semua

(d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; (e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sembilan (9) megabait (MB) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah sangat disarankan; (f) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; (g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; (h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; (i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan (k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; (l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan (m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing. (n) Maklumat lanjut mengenai keselamatan e-mel bolehkah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajun “Garis panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.	Semua

0609 Perkhidmatan E-Usahawan	
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
060901 E-Usahawan	
Bagi menggalakkan pertumbuhan e-usahawan serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-usahawan perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua

060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua
0610 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061001 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT KEDA; (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan	ICTSO

(h) Aktiviti penukaran alamat IP (IP address) selain daripada yang telah diperuntukkan tanpa kebenaran Unit ICT.	
061002 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT
061003 Sistem Log	
(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	

(b) Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Semua
061004 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dilindungi daripada diubahsuai dan sebarang capaian yand tidak dibenarkan; (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan (f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KEDA atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pentadbir Sistem ICT

BIDANG 07

KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

Objektif :

Mengawal capaian ke atas maklumat.

070101 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	Unit ICT, ICTSO

0702 Pengurusan Capaian Pengguna

Objektif :

Mengawal capaian pengguna ke atas aset ICT KEDA.

070201 Akaun Pengguna

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:	Semua

(a) Akaun yang diperuntukkan oleh KEDA sahaja boleh digunakan; (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Akaun pengguna yang di wujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan KEDA. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (f) Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut; i. Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) bulan; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan	Semua
070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
070203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KEDA seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;	Pentadbir Sistem ICT

(b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; (d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan sistem pengoperasian dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; (g) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (i) Menamatkan sesebuah sesi secara automatik yang tidak aktif sekiranya tidak digunakan bagi satu tempoh 10 Minit yang ditetapkan (auto log-off); (j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan (k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	Semua
070204 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya : Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-	Pentadbir Sistem ICT

(a) Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; dan (b) Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci. (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Semua
0703 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian diantara rangkaian KEDA, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem ICT, ICTSO
070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di KEDA hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian KEDA; (b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	Pentadbir Rangkaian, ICTSO, Semua

(c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; (d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; (e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengurus Besar KEDA/ pegawai yang diberi kuasa; (f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; (g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pegawai Bertanggungjawab sebelum dimuat naik ke Internet; (h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; (i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KEDA; (j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti forum, blog dan laman media sosial. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; (k) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan (l) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan	Pentadbir Rangkaian, ICTSO, Semua

ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
0704 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; dan (c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Mengehadkan dan mengawal penggunaan program; dan (d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	Pentadbir Rangkaian, ICTSO, Semua

0705 Kawalan Capaian Aplikasi dan Maklumat	
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
070501 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (*log*) bagi mengesan aktiviti-aktiviti yang tidak diingini; (c) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalah gunaan; (d) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (e) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (f) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimana pun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Semua
0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif : Memastikan keselamatan maklumat apabila menggunakan peralatan mudah alih dan kerja jarak jauh.	

070601 Penggunaan Peralatan Mudah Alih	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Merekodkan aktiviti keluar masuk penggunaan peralatan komputer (b) Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
070602 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

BIDANG 08

PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif :

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

080101 Keperluan Keselamatan Sistem Maklumat	
(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 dan output bagi memastikan program dan hasil data berjalan dengan betul, tepat dan sempurna. (c) Aplikasi perlu mengandungi semakan pengesahan (validation) untuk mengelak sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan. (d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Unit ICT, ICTSO
080102 Pengesahan Data Input dan Output	
(a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian. (b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT

0802 Kawalan Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	Semua
080201 Enkripsi	
Pentadbir Sistem ICT hendaklah membuat enkripsi ke atas maklumat sesitif atau maklumat rahsia pada setiap masa.	Pentadbir Sistem ICT
080202 Pengurusan Username dan Password yang berkesan	
Memastikan bahawa setiap pengguna yang dipertanggungjawabkan dengan Username dan Password supaya dapat melindunginya dari diubah, dimusnah atau didedah sepanjang tempoh sah Username dan Password tersebut.	Semua
0803 Keselamatan Fail Sistem	
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan. (b) Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji. (c) Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. (d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan. (e) Membuat pendua (backup) bagi aturcara dan data-data berkaitan mengikut kekerapan yang dirancang.	Pentadbir Sistem ICT

0804 Keselamatan dalam Proses Pembangunan dan Proses Sokongan	
Sokongan Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 Prosedur Kawalan Perubahan	
(a) Perubahan atau pengubahansuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum dipakai. (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. (c) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan. (d) Menghalang sebarang peluang untuk membocor maklumat.	Pentadbir Sistem ICT
080402 Pembangunan Perisian Secara Outsource	
(a) Pembangun perisian secara out source perlu diselia dan dipantau oleh pemilik sistem. (b) Kod sumber (source code) bagi semua aplikasi dan perisian adalah menjadi hak milik KEDA yang bertanggungjawab.	ICT dan Pentadbir Sistem ICT
0805 Kawalan Teknikal Keterdedahan (Vulnerability)	
Objektif : Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080501 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan.	Pentadbir Sistem ICT

(b)	Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi.	
(c)	Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan adalah menjadi hak milik KEDA berkenaan.	

BIDANG 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif :

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

090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah *(adverse event)* yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CERT KEDA dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	Semua

0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif : Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KEDA. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	Pentadbir Sistem ICT

BIDANG 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

Objektif :

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

100101 Pelan Kesinambungan Perkhidmatan

Pelan kesinambungan perkhidmatan (*Business Continuity Management, BCM*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (f) Membuat penduaan; dan (g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	Semua

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkaraperkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel KEDA dan vendor berserta nombor yang bolehdihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya 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 di mana boleh. Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. KEDA hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	Semua

BIDANG 11

PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif :

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT KEDA.

110101 Pematuhan Dasar

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

110103 Pematuhan Keperluan Audit

Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	Semua

Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	
110104 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua Semua pengguna di KEDA adalah seperti di Lampiran 2	Semua
110105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT KEDA boleh dikenakan tindakan tatatertib.	Semua

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	*Backup* Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	Chief Information Officer Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian penggunayang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft / espionage*), penipuan (*hoaxes*).
GCERT	Government Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.

Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan komunikasi.
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
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.
Intrusion DetectionSystem (IDS)	Sistem Pengesan Pencerobohan
	Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention	Sistem Pencegah Pencerobohan
System (IPS)	Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.

Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
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.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.

Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.

Lampiran 1

AKUAN PEMATUHAN
DASAR KESELAMATAN ICT (DKICT)
LEMBAGA KEMAJUAN WILAYAH KEDAH (KEDA)
VERSI 3.0

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Jabatan/Agensi/Bahagian/Unit : ……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam DKICT Lembaga Kemajuan Wilayah Kedah (KEDA) Versi 3.0; dan

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

Tandatangan : .....

Tarikh : .....

Pengesahan

.....
Ketua Pegawai Maklumat (CIO)
Lembaga Kemajuan Wilayah Kedah (KEDA)

Lampiran 2

SENARAI PERUNDANGAN DAN PERATURAN

a. Arahan Keselamatan;
b. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
c. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
d. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
f. Akta Tandatangan Digital 1997;
g. Akta Rahsia Rasmi 1972;
h. Akta Jenayah Komputer 1997;
i. Akta Hak Cipta (Pindaan) Tahun 1997;
j. Akta Komunikasi dan Multimedia 1998;
k. Perintah-Perintah Am;
l. Arahan Perbendaharaan;fg
m. Arahan Teknologi Maklumat 2007;
n. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
o. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.
p. Surat Pekeliling Am Bilangan 3 Tahun 2015 – Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam;

Ruangan Ini Di Biarkan Kosong