PELABUHAN KUANTAN
MALAYSIA

KAEDAH KESELAMATAN ICT

LEMBAGA PELABUHAN KUANTAN

TERBITAN 2

KANDUNGAN

	0703-KAWALAN CAPAIAN RANGKAIAN	
	070301-CAPAIAN RANGKAIAN	
	070302-CAPAIAN INTERNET	
	070303-CAPAIAN JARAK JAUH	
	0704-KAWALAN CAPAIAN SISTEM PENGOPERASIAN	
	070401-CAPAIAN SISTEM PENGOPERASIAN	
	070402-KAD PINTAR	
	0705-KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT	
	070501-CAPAIAN APLIKASI DAN MAKLUMAT	
	0706-PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH	
	070601-PERALATAN MUDAH ALIH	
	070602-KERJA JARAK JAUH	
12	BIDANG 08 - PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	76
	0801-KESELAMATAN DALAM MEMBANGUNKAN SISTEM DAN APLIKASI	
	080101-KEPERLUAN KESELAMATAN SISTEM APLIKASI	
	080102-PENGESAHAN DATA INPUT	
	080103-PENGESAHAN DATA OUTPUT	
	0802-KAWALAN KRIPTOGRAFI	
	080201-PENYULITAN	
	080202-TANDATANGAN DIGITAL	
	080303-PENGURUSAN INFRASTRUKTUR KUNCI AWAM (PKI)	
	0803-KESELAMATAN FAIL SISTEM	
	080301-KAWALAN FAIL SISTEM	
	0804-KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN	
	080401-PROSEDUR KAWALAN PERUBAHAN	
	080402-PEMBANGUNAN SECARA OUTSOURCE	
	0805-KAWALAN TEKNIKAL KETERDEDAHAN (VULNERABILITY)	
	080501-KAWALAN DARI ANCAMAN TEKNIKAL	

PENGENALAN

Kaedah Keselamatan ICT Lembaga Pelabuhan Kuantan (DKICT LPKtn) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Kaedah ini diguna pakai oleh LPKtn.

Kaedah ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT.

Kaedah ini adalah berdasarkan panduan Dasar Keselamatan ICT yang dikeluarkan oleh pihak MAMPU.

OBJEKTIF

DKICT LPKtn diwujudkan untuk menjamin kesinambungan urusan LPKtn dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama DKICT LPKtn ialah seperti berikut:

(a) Memastikan kelancaran operasi LPKtn dan meminimumkan kerosakan atau kemusnahan;

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

(c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN KAEDAH

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) Memastikan 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.

DKICT LPKtn merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan ketersediaan 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 LPKtn terdiri daripada manusia, peralatan, perisian, telekomunikasi, kemudahan ICT dan data. DKICT LPKtn 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, DKICT LPKtn ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT. 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 agensi. 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 LPKtn;

(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.

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 agensi. Contoh : Sistem dokumentasi, prosedur operasi, rekod-rekod agensi, 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 agensi bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

(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 DKICT LPKtn 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, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa kesemasa 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 di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pembangunan, 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

DKICT LPKtn 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.

BIDANG 01 - PEMBANGUNAN DAN PENYELENGGARAAN KAEDAH

0101 Kaedah Keselamatan ICT

Objektif: DKICT LPKtn diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran pelaksanaan operasi secara berterusan dan meminimumkan kerosakan atau kemusnahan aset ICT.

KENYATAAN	TINDAKAN
010101 Pelaksanaan Kaedah Ketua Jabatan bertanggungjawab dalam memastikan pelaksanaan DKICT dengan cekap dan berkesan dibantu oleh Jawatankuasa ICT (JKICT) LPKtn atau jawatankuasa yang setara dengannya.	Ketua Jabatan
010102 Penyebaran Kaedah Kaedah ini perlu disebarkan kepada semua pengguna LPKtn (termasuk kakitangan, pembekal, pakar runding dan lain-lain)	ICTSO
010103 Penyelenggaraan Kaedah DKICT LPKtn adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, polisi Kerajaan dan kepentingan sosial.	ICTSO

Berikut adalah prosedur penyelenggaraan DKICT LPKtn: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemukakan cadangan pindaan secara bertulis kepada CIO LPKtn untuk dibentangkan dalam Mesyuarat JKICT LPKtn atau mesyuarat yang setara dengannya; (c) Perubahan yang telah dipersetujui oleh JKICT LPKtn atau jawatankuasa yang setara dengannya dimaklumkan kepada semua pengguna LPKtn; dan (d) Kaedah ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
010104 Pengecualian Kaedah DKICT LPKtn adalah terpakai kepada semua pengguna LPKtn dan tiada pengecualian diberikan.	Semua

BIDANG 02 - ORGANISASI KESELAMATAN

Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur_dalam mencapai objektif DKICT LPKtn.

020101 Ketua Jabatan

Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut:

(a) Memastikan semua pengguna mematuhi peruntukan-peruntukan di bawah DKICT LPKtn;

(b) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan

(d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT LPKtn.

020102 Ketua Pegawai Maklumat (CIO)

Jawatan Ketua Pegawai Maklumat (CIO) peringkat LPKtn adalah disandang Pengurus Korporat dan Pembangunan.

Peranan dan tanggungjawab CIO adalah seperti berikut:

(a) Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;

(b) Menentukan keperluan keselamatan ICT;

(c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT LPKtn serta pengurusan risiko dan pengauditan; dan

(d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT LPKtn.

020103 Pegawai Keselamatan ICT (ICTSO)

Jawatan ICTSO bagi peringkat Lembaga Pelabuhan Kuantan adalah disandang oleh Penolong Pengurus Teknologi Maklumat (PK(IT)).

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

(a) Merancang, mengurus dan melaksanakan program keselamatan ICT LPKtn;

(b) Menguatkuasakan pelaksanaan DKICT LPKtn;

(c) Memberi penerangan dan pendedahan berkenaan DKICT LPKtn kepada semua pengguna;

(d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT LPKtn;

(e) Menjalankan pengurusan risiko;

(f) Mengambil tindakan pembetulan ke atas hasil penemuan audit;

(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) LPKtn dan memaklumkannya kepada Pengurus ICT;

(i) Mengenal pasti punca ancaman atau insiden keselamatan ICT dan melaksanakan langkah-langkah baik pulih dengan segera; dan

020104 Pengurus ICT

Pengurus ICT bagi peringkat LPKtn adalah disandang oleh Ketua Unit IT / Pegawai yang bertanggungjawab ke atas ICT. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

(a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan semasa;

(b) Menentukan kawalan akses pengguna terhadap aset ICT LPKtn ;

(c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO LPKtn;

(d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT LPKtn.

020105 Pentadbir Sistem ICT

Pentadbir Sistem ICT di LPKtn disandang oleh Penolong Pegawai Teknologi Maklumat 1 dan Penolong Pegawai Teknologi Maklumat 2.

Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut:

(a) Mengambil tindakan segera apabila kakitangan berhenti, bertukar, bercuti, berkursus panjang 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 DKICT LPKtn;

(c) Memantau aktiviti capaian harian pengguna;

(d) Memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik;

(e) Mengenal pasti aktiviti-aktiviti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan segera;

(f) Menyimpan dan menganalisis rekod jejak audit;

(g) Menyediakan laporan mengenai aktiviti capaian secara berkala.

020106 Pengguna

Peranan dan tanggungjawab pengguna adalah seperti berikut:

(a) Membaca, memahami dan mematuhi DKICT LPKtn;

(b) Mengetahui dan memahami kesan tindakannya terhadap keselamatan ICT.

(c) Lulus tapisan keselamatan;

(d) Melaksanakan prinsip-prinsip DKICT LPKtn;

(e) Menjaga kerahsiaan maklumat LPKtn ;

(f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;

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

(h) Menandatangani "Aku Janji Pematuhan Kaedah Keselamatan LPKtn" bagi mematuhi DKICT LPKtn.

020107 Jawatankuasa Mesyuarat ICT (JPICT) LPKtn

Jawatankuasa Mesyuarat ICT (JPICT) LPKtn adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT LPKtn.

Keanggotaan Ahli **Jawatankuasa Mesyuarat JPICT LPKtn** adalah seperti berikut:

Pengerusi: Pengurus Besar

Ahli : Pengurus Korporat dan Pembangunan

Pengurus Operasi dan Kawalselia

Pengurus Kewangan Dan Pentadbiran

Penolong Pengurus (Teknologi Maklumat)

Penolong Pegawai Teknologi Maklumat I

Penolong Pegawai Teknologi Maklumat II

Urus setia: Unit IT

Bidang kuasa:

(a) Memperakukan / meluluskan dokumen DKICT LPKtn;

(b) Memantau tahap pematuhan keselamatan ICT;

(c) Menilai aspek teknikal keselamatan projek-projek ICT;

(d) Memperakukan dan meluluskan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT LPKtn;

(e) Memastikan sistem ICT sentiasa mematuhi keperluan keselamatan dari semasa ke semasa;

(f) Memberi nasihat kepada JPICT dari aspek keselamatan ICT;

(g) Menilai kesesuaian teknologi untuk keperluan keselamatan ICT;

(h) Memastikan DKICT LPKtn selaras dengan dasar-dasar ICT kerajaan semasa;

(i) Membincangkan laporan keselamatan ICT dan menyelesaikan isu-isu berbangkit;

(j) Menimbang dan meluluskan Pelan Kesinambungan Perkhidmatan (BCP) LPKtn.

(k) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden; dan

(l) Membincangkan pelanggaran DKICT LPKtn dan tindakan yang perlu diambil.

020108 Pasukan Tindak Balas Insiden Keselamatan ICT LPKtn (HelpDesk ICT)

Keanggotaan CERT LPKtn adalah seperti berikut:

Keahlian di Peringkat LPKtn

Pengarah : CIO LPKtn

Pengurus : ICTSO LPKtn

Urus setia: Penolong Pegawai Teknologi Maklumat di Unit IT, LPKtn

Keahlian CERT di Peringkat Jabatan

Pengarah : CIO Jabatan

Pengurus : ICTSO Jabatan

Ahli :

- Pegawai Teknologi Maklumat
- Penolong Pegawai Teknologi Maklumat

Urus setia: Unit IT

Bagi Jabatan/Agensi yang tidak mempunyai kakitangan Teknologi Maklumat yang mencukupi, CERT Jabatan tidak perlu diwujudkan dan sebarang insiden keselamatan ICT hendaklah dilaporkan terus kepada CERT di peringkat Kementerian.

Peranan dan tanggungjawab Unit IT LPKtn adalah seperti berikut:

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

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

(c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;

(d) Menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama

ada sebagai input atau untuk tindakan seterusnya;

(e) Menasihati LPKtn mengambil tindakan pemulihan dan pengukuhan;

(f) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada pengguna LPKtn; dan

(g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.

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) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;

(b) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna;

(c) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga.

(d) Perkara-perkara yang perlu dimasukkan dalam perjanjian hendaklah selaras dengan :

i. DKICT LPKtn;
ii. Arahan Keselamatan;

iii. Perakuan Akta Rahsia Rasmi 1972; dan

iv. Hak Harta Intelek.

(e) Menandatangani "Aku Janji Pematuhan Kaedah Keselamatan LPKtn" bagi mematuhi DKICT LPKtn

Tindakan oleh: CIO, ICTSO,Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

BIDANG 03 - PENGURUSAN ASET ICT

0301 Akauntabiliti Aset

Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT LPKtn.

030101 Inventori Aset ICT

Kenyataan	Tindakan
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkodkan 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) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di LPKtn; (d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan (e) Setiap pengguna adalah bertanggungjawab ke atas aset ICT dibawah kawalannya.	Pentadbir Sistem, Pegawai Aset dan semua pengguna LPKtn

0302 Pengelasan dan Pengendalian Maklumat

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

030201 Pengelasan Maklumat

Kenyataan	Tindakan
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh Pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	Pegawai Pengelas

030202 Pengendalian Maklumat

Kenyataan	Tindakan
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan,menghantar, menyampai, menukar dan memusnahkan 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,Pegawai Pengelas

BIDANG 04 : KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

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

040101 Sebelum Perkhidmatan

Kenyataan	Tindakan
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua pengguna dan pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan tatacara 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 berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

040102 Dalam Perkhidmatan

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua pengguna serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan garis panduan dan peraturan serta perundangan berkaitan yang ditetapkan ; (b) memberi kesedaran mengenai pengurusan keselamatan aset ICT yang berkaitan diberi 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 sekiranya perlu ke atas semua pengguna, pembekal, pakar runding dan pihak ketiga yang berkepentingan apabila berlaku perlanggaran dengan perundangan dan peraturan ditetapkan; 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.	Semua

040103 Bertukar Atau Tamat Perkhidmatan

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada Pegawai Aset mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan dan/atau terma perkhidmatan.	

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

Kenyataan	Tindakan
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 dikenal 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) Memastikan alat penggera atau kamera sentiasa berfungsi dengan baik mengikut keperluan; (d) Memastikan kaunter kawalan dan perkhidmatan keselamatan diwujudkan serta menghadkan jalan keluar masuk bagi memastikan pengguna yang dibenarkan sahaja memasuki kawasan tersebut;	Pegawai Keselamatan, CIO dan ICTSO

(e) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; (f) Mereka bentuk dan melaksanakan susun atur keselamatan fizikal di dalam ruang pejabat yang mempunyai kemudahan ICT; (g) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana (*force majeure*);	

050102 Kawalan Masuk Fizikal

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Semua pengguna hendaklah memakai dan mempamerkan pas keselamatan sepanjang waktu bertugas; (b) Pas keselamatan hendaklah dikembalikan apabila pengguna tidak lagi berkhidmat di LPKtn; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter kawalan keselamatan dan hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan kadar segera kepada pihak yang mengeluarkannya.	Semua

050103 Kawasan Larangan

Objektif: Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut.

Kenyataan	Tindakan
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Perkara-perkara yang perlu dipatuhi di kawasan larangan adalah seperti berikut: (a) Akses kepada kawasan larangan hanyalah kepada pegawai pegawai yang dibenarkan sahaja; dan (b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas dikawasan berkenaan selesai.	

0502 Keselamatan Peralatan

Objektif : Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.

050201 Peralatan ICT

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (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, menanggalkan atau menukar ganti sebarang perkakasan ICT yang telah ditetapkan tanpa kebenaran; (d) pengguna dilarang membuat sebarang pemasangan *(installation)* perisian tanpa kebenaran Pentadbir Sistem atau pegawai yang dipertanggungjawabkan ; (e) pengguna mestilah memastikan perisian *antivirus* di komputer mereka dikemas kini dan sentiasa melakukan imbasan ke atas media storan yang digunakan; (f) semua peralatan sokongan ICT hendaklah dilindungi daripada dicuri,dirosakkan, disalah guna dan diubahsuai tanpa kebenaran; (g) setiap pengguna adalah bertanggungjawab ke atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;	

(h) peralatan-peralatan kritikal perlu dibekalkan dengan *Uninterruptable Power Supply* (UPS);

(i) semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switch, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

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

(k) peralatan ICT yang hendak dibawa keluar dari premis agensi, perlulah mendapat kelulusan dan direkodkan bagi tujuan pemantauan;

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

(m) pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

(n) pengguna tidak dibenarkan memindahkan peralatan ICT dari tempat asal tanpa kebenaran pegawai yang dipertanggungjawabkan;

(o) sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaikpulih;

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

(q) pengguna bertanggungjawab terhadap perkakasan, perisian

serta maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; dan (r) Pengguna hendaklah mematikan suis semua perkakasan ICT apabila meninggalkan pejabat.	

050202 Media Storan

Kenyataan	Tindakan
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik,selamat, terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan. Bagi menjamin keselamatan, perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (b) bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu; (c) semua data di dalam media storan yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat; (d) semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang	semua

mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (e) media storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; (f) media *backup* hendaklah diletakkan di tempat yang terkawal;dan (g) membuat salinan atau penduaan (data *backup*) bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.	

050203 Media Tandatangan Digital

Kenyataan	Tindakan
Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut: (a) Pegawai hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah-milik atau dipinjamkan; dan (c) sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya	Semua

050204 Media Perisian dan Aplikasi

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang sah sahaja dibenarkan bagi kegunaan LPKtn; (b) sebarang instalasi perisian selain daripada perisian *pre-installed* oleh Unit IT hendaklah mendapatkan kebenaran bertulis daripada CIO atau pegawai yang bertanggungjawab; (c) sistem aplikasi dalaman tidak dibenarkan diagih/didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (d) 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 (e) *source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua, Pengurus ICT

050205 Penyelenggaraan Perkakasan

Kenyataan	Tindakan
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti.	

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Bertanggungjawab terhadap penyelenggaraan setiap perkakasan ICT sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (b) semua perkakasan yang di selenggara hendaklah mematuhi spesifikasi yang telah ditetapkan; (c) memastikan perkakasan hanya di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (d) menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT atau pegawai yang bertanggungjawab.	

050206 Peralatan di Luar Premis

Kenyataan	Tindakan
Perkakasan yang dibawa keluar dari premis adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; (b)Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua

050207 Pelupusan Perkakasan

Kenyataan	Tindakan
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak ekonomik untuk dibaiki sama ada harta modal atau inventori yang dibekalkan.	
Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat yang terdapat di dalam aset ICT tidak terlepas dari kawalan.	Pegawai Aset, Unit IT
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan data-data dalam storan telah dihapuskan dengan cara yang selamat sebelum peralatan ICT dilupuskan; (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan (c) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (d) peralatan yang hendak di lupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (e) Pegawai aset bertanggungjawab merekodkan butir – butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistemyang diguna pakai; (f) pelupusan peralatan ICT hendaklah dilakukan secara	Semua

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. Menanggalkan dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM, Hardisk, motherboard* dan sebagainya;

ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di LPKtn;

iii. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan;

iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab LPKtn ; dan

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

0503 Keselamatan Persekitaran

Objektif: Melindungi aset ICT dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

050301 Kawalan Persekitaran

Kenyataan	Tindakan
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 Pengurus Besar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (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 (pemadam api, pengesan kebakaran dan sebagainya) hendaklah berfungsi dan diletakkan di tempat yang bersesuaian, mudah dicapai dan dikendalikan; (d) bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (e) semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; dan	Semua

(f) pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer.	

050302 Bekalan Kuasa

Kenyataan	Tindakan
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (b) peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*gen-set*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; (c) semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Bahagian/ Unit IT, ICTSO, Semua

050303 Kabel Rangkaian

Kenyataan	Tindakan
Kabel rangkaian hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada	Bahagian/ Unit IT, ICTSO,

kerosakan dan pintasan maklumat; (b) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi Mengelakkan ancaman kerosakan dan *wire tapping*; dan (d) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan.	

0504 Keselamatan Dokumen

Objektif: Melindungi maklumat dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

050401 Dokumen

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (b) kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (c) pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (d) menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua

BIDANG 06 - PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur Operasi

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

060101 Pengendalian Prosedur

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur keselamatan ICT yang di wujud, 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 pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua

060102 Kawalan Perubahan

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggarakan, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan oleh pegawai atasan atau pemilik aset ICT; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua

060103 Pengasingan Tugas dan Tanggungjawab

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahan yang tidak dibenarkan ke atas aset ICT; (b) 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 di manipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian jika perlu.	Pengurus ICT, 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.

060201 Perkhidmatan Penyampaian

Kenyataan	Tindakan
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pihak ketiga; (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (c) Pengurusan ke atas perubahan kaedah perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian risiko.	Bahagian/ Unit IT, ICTSO, Semua

0603 Perancangan dan Penerimaan Sistem

Objektif :

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

060301 Perancangan Kapasiti

Kenyataan	Tindakan
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT, ICTSO

060302 Penerimaan Sistem

Kenyataan	Tindakan
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT, 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

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (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 perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya dan secara berkala; (d) Mengemas kini antivirus dengan *pattern* antivirus yang terkini ; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi	

mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	

060402 Perlindungan dari *Mobile Code*

Kenyataan	Tindakan
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua

0605 *Housekeeping*

Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

060501 *Backup*

Kenyataan	Tindakan
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah.	Semua

(a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi mengikut prosedur yang telah ditetapkan. Kekerapan *backup* bergantung pada tahap kritikal maklumat; (c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) LPKtn hendaklah menyimpan *backup* mengikut keperluan atau sekurang-kurangnya satu (1) generasi *backup*; dan (e) Merekodkan 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

Kenyataan	Tindakan
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: (a) Semua tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan	Unit IT / Pegawai bertanggung jawab

pengubahsuaian yang tidak dibenarkan;

(b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciriciri 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) *Firewall* hendaklah dipasang serta di konfigurasi dan diselia oleh Pentadbir Sistem;

(e) Semua *tra*fik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan LPKtn;

(f) Semua perisian *sniffer* atau *network analyser, proxy* dan sebarang perisian penggodam adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

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

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

(i) Sebarang penyambungan dan penggunaan rangkaian yang bukan di bawah kawalan LPKtn adalah tidak dibenarkan kecuali dengan kebenaran khas ICTSO;

(j) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.

0607 Pengurusan Media

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

060701 Penghantaran dan Pemindahan

Kenyataan	Tindakan
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua

060702 Prosedur Pengendalian Media

Kenyataan	Tindakan
Di antara prosedur-prosedur pengendalian media termasuk: (a) Melabelkan semua media mengikut tahap keselamatan sesuatu maklumat; (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (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 yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua

0608 Pengurusan Pertukaran Maklumat

Objektif: Memastikan keselamatan pertukaran maklumat dan perisian dengan agensi luar terjamin.

060801 Pertukaran Maklumat

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara LPKtn dengan pihak luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari LPKtn;	Semua

060802 Pengurusan Mel Elektronik (E-mel)

Kenyataan	Tindakan
Penggunaan e-mel di LPKtn hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan tatacara penggunaan e-mel dan Internet yang terkandung dalam Tatacara Penggunaan E-Mel Dan Internet LPKtn.	Semua

0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)

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-Dagang

Kenyataan	Tindakan
Bagi menggalakkan pertumbuhan e-dagang 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-dagang 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

Kenyataan	Tindakan
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 disahkan 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

Kenyataan	Tindakan
ICTSO mestilah bertanggungjawab merekodkan dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT LPKtn (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*);	ICTSO

(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 *bandwidth* rangkaian; (g) aktiviti penyalahgunaan akaun e-mel; dan (h) aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem.	

061002 Jejak Audit

Kenyataan	Tindakan
Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekodkan 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 ciri-ciri 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	Pentadbir Sistem ICT

(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 masa 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.	

061003 Sistem Log

Kenyataan	Tindakan
Pentadbir Sistem hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO, Pengurus ICT dan CIO.	Pentadbir Sistem

061004 Pemantauan Log

Kenyataan	Tindakan
lanya bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya 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 di wujud dan hasilnya perlu dipantau secara berkala; (c) Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti pentadbiran dan operator/pengendali sistem perlu direkodkan; (e) Kesalahan, kesilapan dan / atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya; dan (f) Penyelarasan masa bagi domain keselamatan perlu menggunakan sumber masa yang sama (*time synchronization*). LPKtn menggunakan sumber melalui SIRIM Malaysia (mst.sirim.my) sebagai rujukan utama.	Unit IT / Pegawai bertanggung jawab, Pentadbir Sistem

BIDANG 07 - KAWALAN CAPAIAN

0701 Kaedah Kawalan Capaian

Objektif : Mengawal capaian ke atas maklumat.

070101 Keperluan Kawalan Capaian

Kenyataan	Tindakan
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong kaedah 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 IT / Pegawai bertanggung jawab, ICTSO

0702 Pengurusan Capaian Pengguna

Objektif: Mengawal capaian pengguna ke atas aset ICT.

070201 Akaun Pengguna

Kenyataan	Tindakan
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: (a) akaun yang diperuntukkan oleh LPKtn sahaja boleh digunakan; (b) akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) akaun pengguna yang diwujudkan pertama kali akan diberi hak capaian (*access right*) paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan hak capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (d) pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan LPKtn. 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 dari Kumpulan Sokongan yang bercuti panjang atau menghadiri kursus di luar pejabat dalam	

tempoh waktu melebihi sebulan; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	

070202 Hak Capaian

Kenyataan	Tindakan
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. Hak capaian sistem pengguna perlu disemak setiap 6 bulan	Semua

070203 Pengurusan Kata Laluan

Kenyataan	Tindakan
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 LPKtn seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;	Semua

(b) pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi;

(c) panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (Alphanumerik);

(d) kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

(e) kata laluan *windows* 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 kata laluan diset semula;

(h) kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

(i) tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;

(j) kata laluan hendaklah ditukar selepas tempoh 180 hari atau selepas tempoh masa bersesuaian; dan

(k) Mengelakkan penggunaan semula empat (4) kata laluan yang telah digunakan.

070204 Clear Desk dan Clear Screen

Kenyataan	Tindakan
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; (b) menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	

0703 Kawalan Capaian Rangkaian

Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

070301 Capaian Rangkaian

Kenyataan	Tindakan
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian LPKtn, 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 dan ICTSO

070302 Capaian Internet

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Penggunaan Internet di LPKtn 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 LPKtn;

(b) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

(c) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;

(d) Penggunaan teknologi *packet shaper* untuk mengawal aktiviti (videoconferencing, *video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan;

(e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh pegawai yang diberi kuasa;

(f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

(g) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

(h) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh LPKtn;

(i) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih

dahulu tertakluk kepada Kaedah dan peraturan yang telah ditetapkan; (j) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali kecuali dengan kebenaran khas; dan (k) 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 ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah dan subversif.	

070303 Capaian Jarak Jauh

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah *Remote Access* mestilah menggunakan kaedah penyulitan (*encryption*); (b)Lokasi bagi akses ke sistem ICT LPKtn hendaklah dipastikan selamat; dan (c)Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada CIO/Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Semua

0704 Kawalan Capaian Sistem Pengoperasian

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

070401 Capaian Sistem Pengoperasian

Kenyataan	Tindakan
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer 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 selaras dengan peraturan Jabatan; (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 termasuk berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; (b) mewujudkan satu pengenalan diri (ID) yang unik untuk setiap	Pentadbir Sistem ICT, ICTSO

pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) menghadkan dan mengawal penggunaan program; dan (d) menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	

070402 Kad Pintar

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan kad pintar kerajaan elektronik (Kad EG) hendaklah digunakan bagi capaian sistem kerajaan elektronik yg dikhususkan; (b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain. (c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga(3) kali cubaan akan disekat. (d) Sebarang kehilangan, kerosakan dan kata laluan disekat terhadap kad pintar perlu dimaklumkan kepada pegawai yang dipertanggungjawabkan.	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

Kenyataan	Tindakan
Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di LPKtn adalah terhad kepada pengguna dantujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut hak capaian dan keselamatan maklumat yang telah ditentukan; (b) setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (c) mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (d) memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; (e) capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan	Pentadbir Sistem ICT,ICTSO

(f) sebarang maklumat yang perlu dimuat naik ke portal atau laman web hendaklah mendapat kebenaran daripada pegawai yang dipertanggungjawabkan.	

0706 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh

070601 Peralatan Mudah Alih

Kenyataan	Tindakan
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan	Semua

070602 Kerja Jarak Jauh

Kenyataan	Tindakan
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

BIDANG 08 - PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

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

080101 Keperluan Keselamatan Sistem Aplikasi

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; dan (c) 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.	Pemilik Sistem, Pentadbir Sistem ICT,ICTSO

080102 Pengesahan Data Input

Kenyataan	Tindakan
Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pemilik Sistem dan Pentadbir Sistem ICT

080103 Pengesahan Data Output

Kenyataan	Tindakan
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.

080201 Penyulitan

Kenyataan	Tindakan
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	semua

080303 Pengurusan Infrastruktur Kunci Awam (PKI)

Kenyataan	Tindakan
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

0803 Keselamatan Fail Sistem

Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

080301 Kawalan Fail Sistem

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Proses pengemas kini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan (d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem dan Pentadbir Sistem ICT

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

080401 Prosedur Kawalan Perubahan

Kenyataan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;	Pemilik Sistem dan Pentadbir Sistem ICT

(b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. (c) Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; (d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (e) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan (f) Menghalang sebarang peluang untuk membocorkan maklumat.	

080402 Pembangunan Secara *Outsource*

Kenyataan	Tindakan
Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh pemilik sistem.	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

Kenyataan	Tindakan
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; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

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

Kenyataan	Tindakan
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 kaedah keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO 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 mekanisma kawalan akses: i. hilang, dicuri atau didedahkan; ii. 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 diingini. Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	

0902 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

Kenyataan	Tindakan
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 LPKtn.	

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; (c) menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) menyediakan tindakan pemulihan segera; dan (e) memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

BIDANG 10 - PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Kaedah Kesinambungan Perkhidmatan

Objektif :

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

100101 Pelan Kesinambungan Perkhidmatan

Kenyataan	Tindakan
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 JKICT LPKtn dan perkara-perkara berikut perlu diberi perhatian: (a) mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (c) mendokumentasikan proses dan prosedur yang telah dipersetujui; (d) mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (e) membuat *backup*;	Pengurus ICT

(f) menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali atau mengikut keperluan; dan (g) mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap sistem penyampaian perkhidmatan, bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personal LPKtn dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personal 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. LPKtn hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

BIDANG 11 – PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelakkan sebarang pelanggaran kepada DKICT LPKtn.

110101 Pematuhan Kaedah

Kenyataan	Tindakan
Setiap pengguna LPKtn hendaklah membaca, memahami dan mematuhi DKICT LPKtn dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT LPKtn termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Pegawai yang diturunkan kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT LPKtn selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber LPKtn.	Semua Ketua Jabatan atau pegawai yang diturunkan kuasa

1102 Pematuhan dengan Kaedah, Piawaian dan Keperluan Teknikal

Kenyataan	Tindakan
Memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi kaedah, piawaian dan keperluan teknikal. Sistem ICT perlu diperiksa secara berkala bagi memastikan standard pelaksanaan keselamatan ICT sentiasa dipatuhi.	ICTSO

1103 Pematuhan Keperluan Audit

Kenyataan	Tindakan
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem ICT. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua

1104 Keperluan Perundangan

Kenyataan	Tindakan
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di LPKtn: (a) Arahan Keselamatan; (b) Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "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 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); (e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan"; (f) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; (g) Surat Pekeliling Am Bil. 4 Tahun 2006 – "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam"; (h) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006; (i) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai	Semua

Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh pada 1 Jun 2007; (j) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007; (k) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasajawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan(JITIK); (l) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- "Tatacara Penyediaan, Penilaian dan Penerimaan Tender"; (m) Surat Pekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan"; (n) Akta Tandatangan Digital 1997; (o) Akta Rahsia Rasmi 1972; (p) Akta Jenayah Komputer 1997; (q) Akta Hak cipta (Pindaan) Tahun 1997; (r) Akta Komunikasi dan Multimedia 1998; (s) Perintah-Perintah Am; (t) Arahan Perbendaharaan; (u) Arahan Teknologi Maklumat 2007; (v) Tatacara Penggunaan E-mail dan Internet; (w) *Standard Operating Procedure* (SOP) ICT LPKtn; dan (x) Polisi*, standard, SOP LPKtn/Jabatan yang berkaitan.*	

1105 Pelanggaran Kaedah

Kenyataan	Tindakan
Pelanggaran DKICT LPKtn 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 untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
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.
BCP	*Business Continuity Planning* Pelan tindakan untuk merancang aktiviti-aktiviti kesinambungan perkhidmatan.
CERT	Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
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 atau penyulitan 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 pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft* /

	espionage), penipuan(*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	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 Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
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 Kementerian.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perrkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
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.