DASAR KESELAMATAN ICT

Institut Latihan Kehakiman Dan Perundangan (ILKAP)
Jabatan Perdana Menteri

4 Ogos 2019

Versi 2.2

SEJARAH DOKUMEN

DOKUMEN	VERSI	TARIKH KUATKUASA
DASAR KESELAMATAN ICT ILKAP	1.0	3 JANUARI 2011
DASAR KESELAMATAN ICT ILKAP	2.0	1 MEI 2012
DASAR KESELAMATAN ICT ILKAP	2.1	1 OGOS 2014
DASAR KESELAMATAN ICT ILKAP	2.2	4 OGOS 2019

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) ILKAP. Dasar ini juga menerangkan kepada semua pengguna di ILKAP mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT ILKAP.

OBJEKTIF

Dasar Keselamatan ICT ILKAP diwujudkan untuk menjamin kesinambungan urusan ILKAP dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi ILKAP. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi. Objektif utama Keselamatan ICT ILKAP adalah seperti berikut:

1. Memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT jabatan;
2. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan (*CIA*3);
3. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
4. Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan pembekal;
5. Memperkemaskan pengurusan risiko;
6. Mencegah penyalahgunaan atau kecurian aset ICT jabatan; dan
7. Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

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 ILKAP 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

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti maklumat (contoh: fail, dokumen, data elektronik), perisian (contoh: aplikasi dan sistem perisian) dan fizikal (contoh: komputer, peralatan komunikasi dan media magnet). Dasar ini adalah terpakai oleh semua pengguna di ILKAP termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT ILKAP.

Sistem ICT ILKAP terdiri daripada manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT dan data. Dasar Keselamatan ILKAP telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

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

b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan ILKAP.

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

a) Data dan maklumat

Semua data dan maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT.

b) Peralatan ICT

Semua peralatan komputer dan *peripheral* seperti *server*, *firewall,* komputer peribadi, stesen kerja, kerangka utama, pencetak, peralatan multimedia dan alat-alat prasarana seperti *Uninterruptible Power Supply* (UPS), punca kuasa dan lain-lain;

c) Media storan

Semua media storan dan peralatan yang berkaitan seperti disket, storan mudah alih, kartrij, CD-ROM, pita, cakera, pemacu cakera, pemacu pita dan lain-lain;

d) Media komunikasi

Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway, bridge, router*, peralatan PABX, *wireless* LAN, talian ISDN, peralatan *video conferencing, modem*, PCMCIA, kabel rangkaian, *network interface card* (NIC), *switches, hub* dan lain-lain;

e) 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 ILKAP;

f) Dokumentasi

Semua dokumen (prosedur dan manual pengguna) yang berkaitan dengan aset ICT, pemasangan dan pengoperasian peralatan dan perisian, sama ada dalam bentuk elektronik atau bukan elektronik;

g) Premis Komputer dan Komunikasi

Semua kemudahan serta premis yang diguna untuk menempatkan perkara (a) hingga (h) di atas; dan

h) Manusia

Semua pengguna infrastruktur ICT ILKAP yang dibenarkan, termasuk warga ILKAP, pengguna dan pembekal.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT ILKAP 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 membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah dan membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/ bidang kuasa;

c. Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT ILKAP. 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 mengenalpasti 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 meyimpan log tindakan keselamatan atau *audit trail*;

f. Pematuhan

Dasar Keselamatan ICT ILKAP 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 bergantung

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

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

ILKAP 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 ILKAP termasuklah aplikasi, perisian, perkakasan, pelayan, rangkaian, pangkalan data, sumber manusia, proses dan 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.

ILKAP 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.

ILKAP perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
2. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;

3. Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
4. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

Perkara 04 : Pembangunan dan Penyelenggaraan Dasar

0101 Dasar Keselamatan ICT		
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan ILKAP dan perundangan yang berkaitan.		
010101 Pelaksanaan Dasar		
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah (KP), dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Program.	KP
010102 Penyebaran Dasar		
	Dasar ini perlu disebarkan kepada semua pengguna ILKAP (termasuk kakitangan, pembekal, pakar runding dll.)	ICTSO
010103 Penyelenggaraan Dasar		
	Dasar Keselamatan ICT ILKAP sentiasa disemak dan dipinda dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT ILKAP: a. mengenalpasti dan menentukan perubahan yang diperlukan; b. mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatan Kuasa Pemandu ICT (JPICT);	ICTSO

	c. perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan d. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	
010104	**Pengecualian Dasar**	
	Dasar Keselamatan ICT ILKAP adalah terpakai kepada semua pengguna ICT ILKAP dan tiada pengecualian diberikan.	Semua

Perkara 02 : Organisasi Keselamatan

0201 Infrastruktur Organisasi Keselamatan		
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.		
020101 Ketua Pengarah (KP)		
	Peranan dan tanggungjawab KP adalah seperti berikut : a. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT ILKAP; b. memastikan semua pengguna mematuhi Dasar Keselamatan ICT ILKAP; 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 ILKAP.	KP
020102 Ketua Pegawai Maklumat (CIO)		
	Pendaftar (Bahagian Pengurusan) ILKAP adalah Ketua Pegawai Maklumat (CIO). Peranan dan tanggung jawab beliau adalah seperti berikut : a. membantu KP dalam melaksanakan tanggung jawab menjaga keselamatan aset ICT berdasarkan Dasar Keselamatan ICT; b. menentukan keperluan keselamatan ICT; dan	CIO

	c. membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT seperti penyediaan DKICT ILKAP serta pengurusan risiko dan pengauditan; dan d. bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT ILKAP.	
020103	**Pegawai Keselamatan ICT (ICTSO)**	
	Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut : a. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT ILKAP; b. menguatkuasakan pelaksanaan Dasar Keselamatan ICT ILKAP; c. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT ILKAP kepada semua pengguna; d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT ILKAP; e. menjalankan pengurusan risiko; f. menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. memberi amaran terhadap kemungkinan berlakunya ancaman merbahaya 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 (GCERT), MAMPU dan memaklumkannya kepada CIO;	ICTSO

	i. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT ILKAP dan memperakukan langkah-langkah baik pulih dengan segera; j. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT ILKAP; k. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan l. menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT agar insiden baru dapat dielakkan.	
020104 Pengurus ICT		
	Timbalan Pendaftar Teknologi Maklumat merupakan Pengurus ICT ILKAP. Peranan dan tanggungjawab beliau adalah seperti berikut : a. membaca, memahami dan mematuhi Dasar Keselamatan ICT ILKAP; b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan ILKAP; c. menentukan kawalan akses semua pengguna terhadap aset ICT ILKAP; d. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan e. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT ILKAP.	Pendaftar BP
020105 Pentadbir Sistem ICT		

	Pegawai Teknologi Maklumat di Bahagian Pengurusan (BP) adalah merupakan Pentadbir Sistem ICT ILKAP. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut : a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, berkurusus 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 Dasar Keselamatan ICT ILKAP; c. memantau aktiviti capaian harian pengguna; d. mengenal pasti aktiviti-aktiviti yang 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 aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; dan g. bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	BP
020106	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti berikut :	Pengguna

a. membaca, memahami dan mematuhi Dasar Keselamatan ICT ILKAP;
b. mengetahui dan memahami implikasi keselamatan ICT, kesan dari tindakannya;
c. lulus tapisan keselamatan;
d. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat ILKAP;
e. melaksanakan langkah-langkah perlindungan seperti berikut:

   i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
   ii. memeriksa maklumat dan menentukan ianya tepat dan lengkap dari masa ke semasa;
   iii. menentukan maklumat sedia untuk digunakan;
   iv. menjaga kerahsiaan kata laluan;
   v. mematuhi standard, prosedur, langkah 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.

f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;
g. menghadiri program-program kesedaran keselamatan ICT; dan
h. menandatangani surat akuan pematuhan Dasar Keselamatan

	ICT ILKAP.	
0202	**Pihak Ketiga**	
Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.		
020201	**Keperluan Keselamatan Kontrak dengan Pihak Ketiga**	
	Akses kepada aset ICT ILKAP perlu berlandaskan kepada perjanjian kontrak. Perkara yang perlu dipatuhi termasuk yang berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT ILKAP; 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 member kebenaran capaian atau penggunaan kepada pihak ketiga; d. akses kepada aset ICT ILKAP 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 dimeteraikan : i. Dasar Keselamatan ICT ILKAP; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan	CIO, ICTSO, Pengurus Komputer, Pentadbir Sistem ICT dan Pihak Ketiga.

	iv. Hak Harta Intelek; f. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT ILKAP sebagaimana di Lampiran 1. Nota 1: Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender" dan Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk "Peraturan Perolehan Perkhidmatan Perundingan" yang berkaitan hendaklah dirujuk.	

Perkara 03 : Kawalan dan Pengelasan Aset

0301 Akauntabiliti Aset

Objektif:

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

030101 Inventori Aset

	Semua aset ICT ILKAP hendaklah direkodkan termasuklah mengenal pasti aset, mengkelaskan aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. 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 dikemaskini; 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 ILKAP; d. Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, didokumen dan dilaksanakan; dan e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem 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 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.	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;	Semua

	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.	

Perkara 04 : Keselamatan Sumber Manusia

0401 Keselamatan Sumber Manusia Dalam Tugas Harian		
Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan ILKAP, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga ILKAP 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 ILKAP serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan ILKAP 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 berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

040102	**Dalam Perkhidmatan**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. memastikan pegawai dan kakitangan ILKAP serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh ILKAP; b. memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT ILKAP 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 undangundang ke atas pegawai dan kakitangan ILKAP serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh ILKAP; 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 Seksyen Teknologi Maklumat Bahagian Pengurusan, ILKAP.	Semua

040103	Bertukar Atau Tamat Perkhidmatan	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. memastikan semua aset ICT dikembalikan kepada ILKAP 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 oleh ILKAP dan/atau terma perkhidmatan.	Semua

Perkara 05 : Keselamatan Fizikal

0501 Keselamatan Kawasan

Objektif:

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

050101 Kawalan Keselamatan

	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Perkara-perkara yang perlu dipatuhi termasuk berikut: a. Kawasan keselamatan fizikal hendalah dikenalpasti 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. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; d. Memperkukuh dinding dan siling; e. Memasang alat penggera atau CCTV; f. Menghadkan jalan keluar masuk; g. Mengadakan kaunter kawalan; h. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; i. Mewujudkan perkhidmatan kawalan keselamatan; j. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO

	kebenaran sahaja boleh melalui pintu masuk ini; k. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; l. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; m. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan n. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102	**Kawalan Masuk Fizikal**	
	Perkara-perkara yang perlu dipatuhi termasuk berikut: a. Setiap pengguna ILKAP hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di Kaunter Pelawat di pintu masuk Bangunan ILKAP. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada ILKAP apabila pengguna berhenti atau bersara; d. Setiap pelawat hendaklah mendaftar di pintu utama ILKAP terlebih dahulu; dan e. Kehilangan pas mestilah dilaporkan dengan segera.	Semua dan Pelawat

050103	**Kawasan Larangan**	
	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. Kawasan larangan di ILKAP adalah bilik Ketua Pengarah, bilik Timbalan Ketua Pengarah, bilik-bilik Pengarah Program, Bilik Server di Pusat Sumber, Bilik Server ITITC, Bilik Server Asrama Eksekutif, Bilik Kawalan CCTV Bangunan Perdana, Bilik Kawalam CCTV ITITC, Bilik Gentian Optik, Bilik PABX dan Stor Penyimpanan Barangan ICT. a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja; b. Secara umumnya, peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu; dan c. 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 di kawasan berkenaan selesai.	Semua
0502	**Keselamatan Peralatan**	
Objektif : Melindungi peralatan dan maklumat ILKAP dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.		

050201 Peralatan ICT

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 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 Pentadbir Sistem 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 disamping 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; i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptible Power Supply* (UPS); j. Semua peralatan ICT hendaklah disimpan atau diletakkan	Semua

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 ILKAP, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;

m. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

p. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem 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 Pentadbir Sistem ICT;

t. Pengguna bertanggungjawab terhadap perkakasan, perisian 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 w. Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
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. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada 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	Semua

	hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e. Akses dan pergerakan media storan hendaklah direkodkan; f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203	**Media Tandatangan Digital**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. Media ini tidak boleh dipindah milik atau dipinjamkan; dan c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Semua

050204	**Media Perisian dan Aplikasi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan ILKAP; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-rom*, *disk* atau media berkaitan bagi mengelakkan 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
050205	**Penyelenggaraan Perkakasan**	
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggara oleh	Pegawai Aset dan Seksyen Teknologi Maklumat, ILKAP

	kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
050206	**Peralatan di Luar Premis**	
	Bagi pekakasan yang dibawa keluar premis ILKAP, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan ILKAP : 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 Perkakasan**	
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh ILKAP dan ditempatkan di ILKAP.	Semua

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan ILKAP. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;

b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;

c. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

d. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

f. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori MyAsset;

g. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

h. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;

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

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

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

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

0503 Keselamatan Persekitaran

Objektif:

Melindungi aset ICT ILKAP dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau 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, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamtan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil : 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 aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g. Semua 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; dan h. Akses kepada saluran *riser* hendaklah dikunci.	Semua

050302	**Bekalan Kuasa**	
	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 *Uninterruptible Power Supply* (UPS) 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.	Seksyen Teknologi Maklumat, ILKAP dan ICTSO
050303	**Kabel**	
	Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan 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; c. Melindungi laluan pemasangan kabel sepenuhnya bagi	Seksyen Teknologi Maklumat, ILKAP dan ICTSO

	mengelakkan ancaman kerosakan, MITM/*wire tapping;* dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
050304	**Prosedur Kecemasan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Arahan Ketua Pengarah Bil. 1 Tahun 2007 : Garis Panduan Kawalan Keselamatan ILKAP; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik oleh Ketua Pengarah ILKAP.	Seksyen Teknologi Maklumat, ILKAP dan ICTSO
0504	**Keselamatan Dokumen**	
Objektif: Melindungi maklumat ILKAP 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,	Semua

	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.	

Perkara 06 : Pengurusan Operasi dan Komunkikasi

0601	**Pengurusan Prosedur Operasi**	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.		
060101	**Pengendalian Prosedur**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
060102	**Kawalan Perubahan**	
	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 asset ICT terlebih dahulu;	Semua

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

	tindakan memisahkan antara kumpulan operasi dan rangkaian.	
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**	
	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**	
	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 dan ICTSO
060302	**Penerimaan Sistem**	
	Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	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**	
	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	Semua

	selamat; b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini anti virus dengan *pattern* antivirus yang terkini; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
060402	**Perlindungan dari *Mobile Code***	
	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***	
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat *backup* 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. 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. Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan e. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Semua
0606	**Pengurusan Rangkaian**	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		

060601	Kawalan Infrastruktur Rangkaian	
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 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 serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan ILKAP; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-	Semua

	aktiviti lain yang boleh mengancam sistem dan maklumat ILKAP; i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan ILKAP adalah tidak dibenarkan; k. Semua pengguna hanya dibenarkan menggunakan rangkaian ILKAP sahaja dan penggunaan modem adalah dilarang sama sekali; dan l. 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**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua
060702	**Prosedur Pengendalian Media**	
	Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitiviti	Semua

	sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak 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.	
060703	**Keselamatan Sistem Dokumentasi**	
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua

0608	Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara ILKAP dan agensi luar terjamin.		
060801	**Pertukaran Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Dasar, 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 ILKAP dengan agensi luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari ILKAP; dan d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
060802	**Pengurusan Mel Elektronik (E-mel)**	
	Penggunaan e-mel di ILKAP hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana-mana undang-undang bertulis yang berkuat kuasa.	Semua

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:

a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh ILKAP 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 ILKAP;

c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

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 sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

g. Pengguna hendaklah mengenal pasti dan mengesahkan identity 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; 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, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan m. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	
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**	
	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:	Semua

	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.	
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 ILKAP; b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), 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 *bandwidth* rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; dan h. Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	ICTSO

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**	

	Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan **c.** Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT
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 diwujud dan hasilnya perlu dipantau secara berkala; 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	Seksyen Teknologi Maklumat, ILKAP dan Pentadbir Sistem ICT

	direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam ILKAP atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

Perkara 07 : Kawalan Capaian

0701 Dasar Kawalan Capaian		
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan asset ICT ILKAP.		
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.	Seksyen Teknologi Maklumat, ILKAP dan ICTSO
0702 Pengurusan Capaian Pengguna		
Objektif : Mengawal capaian pengguna ke atas aset ICT ILKAP.		
070201 Akaun Pengguna		

	Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh ILKAP sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang diwujudkan 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 ILKAP. 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 yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain;	Pentadbir Sistem ICT

	iv. Bersara; atau v. Ditamatkan perkhidmatan.	
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 ILKAP seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus; 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	Pentadbir Sistem ICT

	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. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; j. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan k. Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
070204	***Clear Desk* dan *Clear Screen***	
	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	Semua

	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**	
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian ILKAP, 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**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di ILKAP hendaklah dipantau secara	Pentadbir Rangkaian

	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 ILKAP;	
	b. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	
	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;	Pengurus ICT
	e. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/ pegawai yang diberi kuasa;	Semua
	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 Pengarah Bahagian 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 ILKAP; j. 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 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 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 sistem pengoperasian.		
070401	**Capaian Sistem Pengoperasian**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan	Pentadbir

	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;	Sistem ICT dan ICTSO

	c. Mengehadkan dan mengawal penggunaan program; dan d. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
070402	**Kad Pintar/Kad Magnetik**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan. b. Kad magnetik (*magnetic access door card*) adalah dikhususkan untuk mengakses pintu-pintu utama yang telah ditetapkan oleh Pentadbir Sistem ICT sahaja. Satu unit kad magnetik diberikan kepada setiap pegawai / kakitangan tetap / kontrak di ILKAP bagi membolehkan pergerakan keluar masuk ke ruang pejabat Bahagian / Seksyen / Unit. c. Rekod pengguna dan transaksi penggunaan kad magnetik akan direkodkan di dalam sistem yang disediakan oleh Pentadbir Sistem ICT. d. Pegawai yang bertukar bersara atau bertukar keluar dari ILKAP perlu mengembalikan kad magnetik yang dimiliki kepada Pentadbir Sistem ICT pada hari terakhir bertugas di ILKAP.	Semua

e. Kad pintar dan kad magnetik hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain.

f. 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.

g. Pemilik kad pintar atau kad magnetik perlu membuat laporan polis mengenai kehilangan kad pintar atau kad magnetik. Pemilik kad pintar atau kad magnetik perlu melengkapkan Borang Laporan Insiden Keselamatan (**Lampiran 3**) dan menyerahkannya kepada Pentadbir Sistem ICT dalam tempoh 24 jam dari berlakunya kehilangan tersebut. Borang Laporan Insiden Keselamatan yang lengkap bersama cadangan tindakan susulan oleh Pentadbir Sistem ICT akan dikemukakan kepada Ketua Pengarah ILKAP dan disalinkan kepada Pegawai Keselamatan Jabatan, iaitu Timbalan Ketua Pengarah ILKAP. Pentadbir Sistem ICT akan mengambil tindakan seterusnya sebagaimana diarahkan oleh Ketua Pengarah ILKAP.

h. Dokumen yang diperlukan untuk permohonan kad magnetik baru ialah salinan Borang Permohonan Pas Keselamatan, laporan polis (jika kad magnetik hilang sahaja) serta bayaran kos pentadbiran berjumlah RM20 bagi setiap kad magnetik.

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 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; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem ICT dan ICTSO

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**	
	Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
070602	**Kerja Jarak Jauh**	
	Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

Perkara 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 Maklumat		
	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; c. Aplikasi perlu mengandungi semakan pengesahan (validation) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan 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.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

080102	**Pengesahan Data Input dan Output**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b. Data *output* daripada aplikasi perlu disahkan bagi memastikan 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	**Enkripsi**	
	Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitive atau maklumat rahsia rasmi pada setiap masa.	Semua
080202	**Tandatangan Digital**	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
080203	**Pengurusan Infrastruktur Kunci Awam (*PKI*)**	
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah 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**	
	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 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; d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
0804	**Keselamatan Dalam Proses Pembangunan dan Sokongan**	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
080401	**Prosedur Kawalan Perubahan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pemilik Sistem dan Pentadbir

	a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	Sistem ICT
080402	**Pembangunan Perisian Secara *Outsource***	
	Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik ILKAP.	Seksyen Teknologi Maklumat 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; 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

Perkara 09 : Pengurusan Pengendalian Insiden Keselamatan

0301 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, CERT Agensi dan GCERT MAMPU 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	Semua

	insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di ILKAP sepertimana **Lampiran 2**. 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.		
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 ILKAP. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan	ICTSO

	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.	

Perkara 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 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. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang ditetapkan; c. Mendokumentasikan proses dan prosedur yang telah dipersetujui; d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; e. Membuat penduaan; dan f. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:	ICTSO

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

b. Senarai personel ILKAP dan vendor berserta nombor yang boleh dihubungi (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. ILKAP hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

Perkara 11 : Pematuhan

1101	Pematuhan dan Keperluan Dasar	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT ILKAP.		
110101	**Pematuhan Dasar**	
	Setiap pengguna di ILKAP hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT ILKAP dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua asset ICT di ILKAP 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.	Semua
110102	**Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal**	
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
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	Semua

	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.	
110104	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di ILKAP : 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); d. Pekeliling Am Bilangan 3 Tahun 2001 bertaj k "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. Akta Tandatangan Digital 1997; h. Akta Jenayah Komputer; i. Akta Hak cipta Terpelihara 1997;	Semua

	j. Akta Komunikasi dan Multimedia 1998; k. Arahan Ketua Pengarah Bil. 1 Tahun 2007 : Garis Panduan Kawalan Keselamatan ILKAP; dan l. Arahan Ketua Setiausaha Negara dengan rujukan UPTM (S) 159/338/8 Jilid 30 (34) bertajuk "Langkah-langkah untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Network) di Agensi-agensi Kerajaan"	
110105	**Pelanggaran Dasar**	
	Pelanggaran Dasar Keselamatan ICT ILKAP 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	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 jangkamasa 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 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. Organisasi ini ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.

CERT	*Computer Emergency Response* Team adalah Pasukan Tindak Balas Insiden Keselamatan agensi yang bertindak sebagai *first level support* kepada GCERT MAMPU dalam mengendali insiden keselamatan ICT, mengawasi dan memberi khidmat nasihat berkaitan keselamatan ICT kepada agensi-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 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 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
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.

Lampiran 1

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT ILKAP

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Bahagian : ……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT ILKAP; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : ……

Tarikh : ……

Pengesahan Pegawai Keselamatan ICT ILKAP

……..

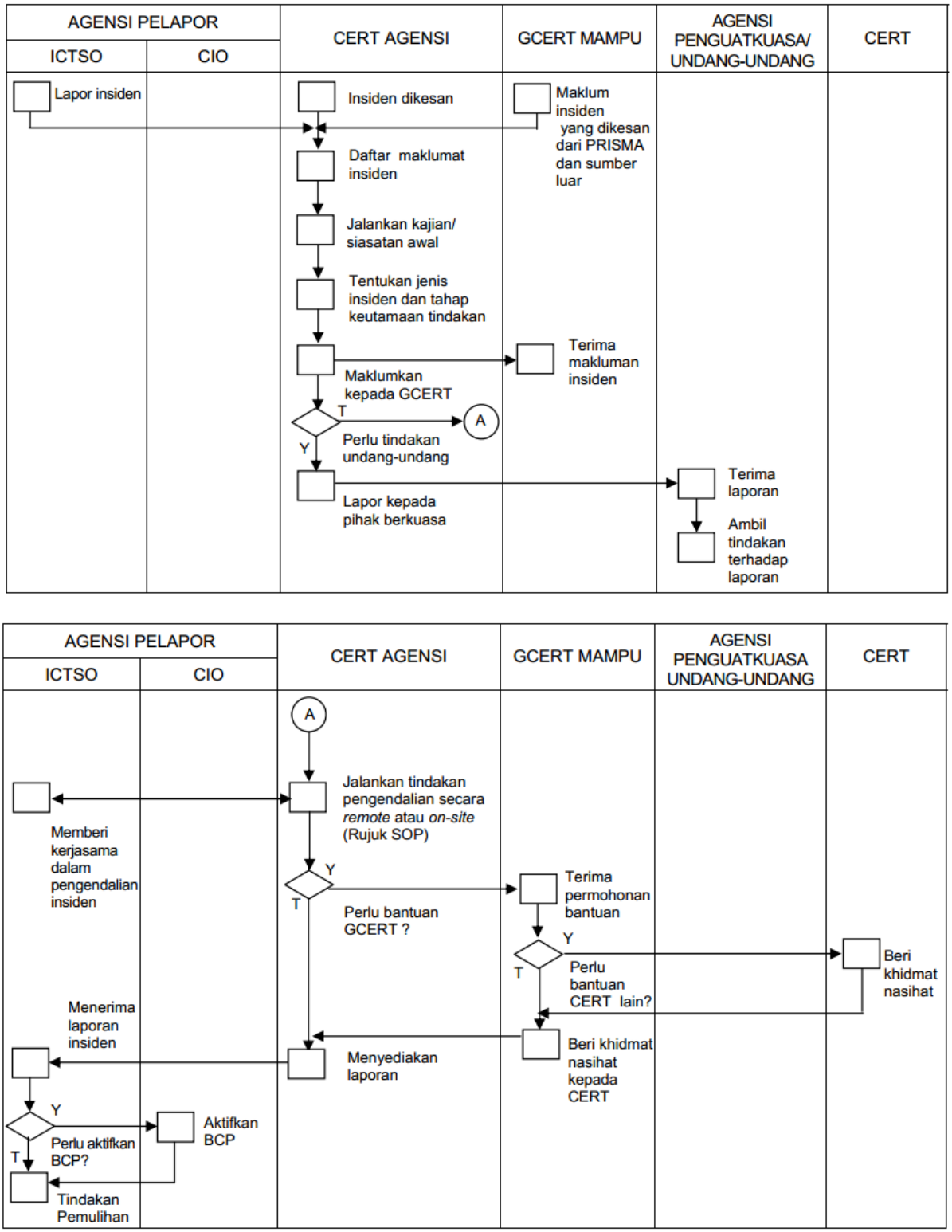
( )

b.p. Ketua Pengarah ILKAP

Tarikh : ……

Lampiran 2

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT ILKAP



Lampiran 3

INSTITUT LATIHAN KEHAKIMAN DAN PERUNDANGAN (ILKAP)

BAHAGIAN PENGURUSAN

BORANG LAPORAN INSIDEN KESELAMATAN ILKAP

BUTIR-BUTIR PENGADU			
Nama Penuh		Jawatan / Gred	
No. Kad Pengenalan		Bahagian / Seksyen / Unit	
Jantina		Aras / Blok	
No. Tel. Pejabat		No. Telefon Bimbit	
MAKLUMAT ADUAN			
Tarikh/ Masa Kejadian		Tempat Kejadian	
*Aduan			

Saya mengaku segala maklumat yang dinyatakan adalah benar.

**Sekiranya ruangan tidak mencukupi sila buat lampiran tambahan.*

Tandatangan Pengadu

KEGUNAAN PEJABAT (PENOLONG PEGAWAI KESELAMATAN FIZIKAL/ICT)			
Tarikh		Masa	
Tindakan Susulan			
Disahkan Oleh : *** Nama dan Cop*		Tandatangan	

ULASAN KETUA JABATAN

Ulasan : _____

Disahkan Oleh : _____

Tandatangan dan Cop Jabatan