LADA

POLISI KESELAMATAN SIBER

LEMBAGA PEMBANGUNAN LANGKAWI

Versi 1.0

DIGITALLYLADA
WE MAKE IT HAPPEN

POLISI KESELAMATAN SIBER
LEMBAGA PEMBANGUNAN LANGKAWI

ISI KANDUNGAN

A. PENGENALAN

Polisi Keselamatan Siber LADA (PKS LADA) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset dan perkhidmatan ICT. Peraturan-peraturan ini perlu difahami dan dipatuhi oleh semua pengguna di LADA. Polisi ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset dan perkhidmatan ICT LADA. Polisi ini adalah terpakai kepada semua kakitangan LADA dan pihak ketiga yang berurusan dengan LADA.

B. OBJEKTIF

PKS LADA diwujudkan untuk memastikan sumber dan penggunaan ICT LADA dapat dikawal selia dan diuruskan dengan cara yang terbaik dan menjamin kesinambungan perkhidmatan LADA dengan meminimumkan kesan insiden keselamatan ICT. Objektif utama keselamatan ICT LADA ialah seperti berikut:

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

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

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

(d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan; dan

(e) Memperkemaskan pengurusan keselamatan ICT LADA.

C. PIAGAM PELANGGAN ICT

(a) Menyelesaikan aduan berkenaan masalah perisian dan sistem selewat-lewatnya dalam tempoh tujuh (7) hari bekerja.

(b) Mengemaskini maklumat yang diterima ke dalam laman web selewat-lewatnya dalam tempoh tiga (3) hari bekerja.

(c) Memastikan aduan mengenai kerosakan peralatan ICT diberi khidmat bantuan sokongan teknikal dalam tempoh 1 hari bekerja setelah laporan diterima.

(d) Menyelesaikan aduan berkenaan masalah talian internet dan jaringan rangkaian dalam tempoh tujuh (7) hari bekerja.

(e) Membangunkan sistem aplikasi khusus selewat-lewatnya dalam tempoh tiga (3) bulan selepas mendapat kelulusan JPICT.

(f) Menyiapkan rekabentuk multimedia dalam tempoh tiga (3) minggu selepas maklumat lengkap diperolehi.

D. PERNYATAAN POLISI

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan merupakan suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan daripada ancaman dan kelemahan yang 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. 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 hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

PKS LADA 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 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 yang sesuai diambil untuk menangani risiko berkenaan.

E. SKOP

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

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

(b) Data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan integriti dan kesahihan maklumat serta untuk melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat; dan

(c) Bagi aset ICT LADA yang ditempatkan di luar premis LADA atau yang disediakan oleh Penyedia Perkhidmatan, hendaklah mengikut aturan/prosedur yang ditetapkan dan diguna pakai oleh Pihak Ketiga/Pemilik Premis/Penyedia Perkhidmatan berkenaan.

Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa, PKS LADA ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dilaksanakan salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan serta prosedur dalam pengendalian semua perkara-perkara berikut:

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan LADA. Contoh: komputer, *server*, peralatan komunikasi dan sebagainya;

(b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan 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 LADA;

(c) Perkhidmatan

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

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

(d) Data dan Maklumat

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

(e) Manusia

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

(f) Premis Komputer dan Komunikasi

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

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

F. PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS LADA 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 dan dibenarkan akses maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan;

(b) Hak Akses Minimum

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

(c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk membolehkan pertanggungjawaban ini dilaksanakan, sistem ICT hendaklah mampu menyokong kemudahan mengesan dan mengesahkan penggunaan sistem ICT.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. Memeriksa data dan maklumat serta menentukan ianya tepat dan lengkap dari semasa ke semasa;

iii. Menentukan data dan 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 daripada diketahui umum.

(d) Pengasingan

Tugas mewujud, memadam, mengemas 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 sistem dan operasi;

(e) Pengauditan

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

(f) Pematuhan

PKS LADA 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 atau pengurusan kesinambungan perkhidmatan; dan

(h) Saling Bergantungan

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

G. PENILAIAN RISIKO KESELAMATAN ICT

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

LADA 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.

LADA hendaklah mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

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

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

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

H. SINGKATAN DAN TAFSIRAN

Berikut ialah jadual singkatan bagi perkataan yang digunakan dalam keseluruhan dokumen ini.

BIL.	SINGKATAN	KETERANGAN
1.	Antivirus	Perisian yang mengimbas virus pada media storan untuk sebarang kemungkinan adanya virus.
2.	API	*Application Programming Interface*
3.	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia
4.	AVR	*Auto Voltage Regulator*
5.	*Backup*	Proses penduaan sesuatu dokumen atau maklumat.
6.	*Bandwidth*	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
7.	BTM	Bahagian Teknologi Maklumat
8.	CDO	*Chief Digital Officer* Ketua Pegawai Digital iaitu merujuk kepada Timbalan Ketua Pegawai Eksekutif (Pengurusan) LADA.

BIL.	SINGKATAN	KETERANGAN
9.	CERT	*Computer Emergency Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT
10.	DDSA	*Data Dictionary* Sektor Awam
11.	*Domain*	Sekumpulan sumber ICT yang terdiri daripada perkakasan dan perisian yang diuruskan di dalam satu persekitaran dengan set peraturan tertentu.
12.	DoS	*Denial of Service* Halangan pemberian perkhidmatan.
13.	E-mel	Elektronik mel
14.	*Encryption*	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
15.	*Firewall*	Peralatan/perisian yang berfungsi untuk mengawal capaian internet dan melindungi sesebuah rangkaian komputer daripada serangan-serangan/pencerobohan oleh pihak luar yang tidak bertanggung jawab.
16.	*Forgery*	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*) dan penipuan (*hoaxes*).
17.	GAMMA	*Gallery of Malaysian Government Mobile Application*
18.	GCERT	*Government Computer Emergency Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan
19.	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
20.	ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
21.	ICTSO	*ICT Security Officer* / Pegawai Keselamatan ICT
22.	IDS	*Intrusion Detection System* 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.

BIL.	SINGKATAN	KETERANGAN
23.	*Internet*	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
24.	*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 rangkaianrangkaian tersebut agar sentiasa berasingan.
25.	IP	*Internet Protocol*
26.	IPS	*Intrusion Prevention System* 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*.
27.	JPICT	Jawatankuasa Pemandu ICT
28.	JTISA	Jawatankuasa Teknikal ICT Sektor Awam
29.	Koordinator ICT Bahagian	Penyelaras atau pegawai yang bertanggungjawab ke atas segala urusan ICT di bahagian di LADA.
30.	Koordinator Web Bahagian	Pegawai yang dilantik dari setiap bahagian dan bertanggungjawab menyemak, memantau dan mengemaskini maklumat di Portal/laman web LADA.
31.	KPE	Ketua Pegawai Eksekutif
32.	LADA	Lembaga Pembangunan Langkawi
33.	LAN	*Local Area Network* Rangkaian Kawasan Setempat
34.	Logout	Log-out komputer / keluar daripada sesuatu sistem atau aplikasi komputer.
35.	*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.
36.	MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia

BIL.	SINGKATAN	KETERANGAN
37.	Modem	*MOdulator DEModulator* Peranti yang boleh menukar bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer
38.	MYCERT	*Malaysia Computer Emergency Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT Malaysia
39.	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
40.	Pentadbir Pusat Data	Pegawai yang bertanggungjawab mengurus dan menyelenggara Pusat Data.
41.	Pembangun Sistem	Pegawai yang bertanggungjawab membangunkan sistem aplikasi.
42.	Pemilik Sistem	Bahagian yang memilik sistem, data dan merupakan pengguna utama sesuatu sistem.
43.	Pengguna	Warga LADA yang dibenarkan menggunakan aset dan perkhidmatan ICT LADA.
44.	Pengurus IT	Pengurus Bahagian Teknologi Maklumat yang bertanggungjawab ke atas urusan ICT di LADA.
45.	Pentadbir Pangkalan Data	Pegawai yang bertanggungjawab mengurus, mengawal, memantau, menyelenggara operasi dan keselamatan pangkalan data.
46.	Pentadbir Rangkaian	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara keselamatan rangkaian.
47.	Pentadbir Sistem Aplikasi	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara sistem aplikasi.
48.	Pentadbir Sistem ICT	Pegawai yang bertanggungjawab mengurus, mengawal, memantau, menyelenggara operasi dan keselamatan server serta data yang disimpan.
49.	Peralatan Rangkaian	*Firewall, switches, server, router*, node rangkaian, *wireless access point*, kabel rangkaian dan *network rack*.
50.	Perisian	Program atau atur cara komputer yang dapat digunakan dengan sistem komputer tertentu. Perisian boleh terdiri daripada perisian sistem atau perisian aplikasi.

BIL.	SINGKATAN	KETERANGAN
51.	Perkakasan ICT	Komponen fizikal yang dihubungkan secara terus dengan komputer atau sistem yang lain. Ia juga merupakan alat yang digunakan sebagai input, dan aktiviti pemprosesan serta output.
52.	PKI	*Public-Key Infrastructure* Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
53.	PKJ	Pegawai Keselamatan Jabatan
54.	PKP	*Business Continuity Management* Pengurusan Kesinambungan Perkhidmatan
55.	*Router*	Peralatan yang menghubungkan beberapa segmen rangkaian komputer yang mempunyai kedudukan rangkaian yang berlainan di dalam WAN.
56.	*Screen Saver*	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
57.	*Server*	Komputer berkapasiti tinggi yang menyediakan pelbagai jenis perkhidmatan untuk diakses oleh lain-lain komputer yang berhubung di dalam rangkaian
58.	Sistem Aplikasi	Perisian yang direkabentuk dan dibangunkan khas untuk kegunaan pengguna komputer yang khusus dan spesifik sama ada yang dibangunkan secara dalaman atau menggunakan perkhidmatan syarikat pembangunan sistem
59.	*Sniffer* atau *Network Analyzer*	Perisian yang digunakan untuk menjejak dan mengesan semua aliran paket data di dalam rangkaian
60.	*Spyware*	Perisian yang membantu dalam mengumpulkan maklumat tentang seseorang atau organisasi tanpa pengetahuan mereka dan yang mungkin menghantar maklumat tersebut kepada entiti lain tanpa persetujuan pengguna, atau yang menimbulkan kawalan ke atas komputer tanpa pengetahuan pengguna.
61.	Switches	Peralatan yang menghubungkan beberapa segmen rangkaian komputer di dalam LAN.

BIL.	SINGKATAN	KETERANGAN
62.	*TCP/IP*	*Transmission Control Protocol/Internet Protocol* yang merupakan standard komunikasi data yang digunakan oleh internet dalam proses pertukaran data dari satu komputer ke komputer lain di dalam jaringan Internet.
63.	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
64.	TKPE(P)	Timbalan Ketua Pegawai Eksekutif (Pengurusan)
65.	UPS	*Uninterruptible Power Supply*
66.	URL	*Universal Resource Location* lokasi atau alamat mana-mana sumber elektronik (dokumen, media dan sebagainya) yang boleh dicapai melalui rangkaian.
67.	*Video Conference*	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
68.	*Video Streaming*	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
69.	*Virus*	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
70.	WAN	*Wide Area Network* Rangkaian Kawasan Luas
71.	*Wireless Access Point*	Peralatan yang membenarkan peralatan tanpa wayar untuk dihubungkan ke rangkaian dengan menggunakan piawaian rangkaian tanpa wayar.
72.	*Worms*	Perisian yang ditulis atau direka khas untuk menyerang sistem rangkaian dan juga komputer peribadi ataupun laptop tanpa menggunakan program untuk menyerang komputer.

I. LAMPIRAN

Lampiran 1 - Surat Akuan Pematuhan Polisi Keselamatan Siber LADA
Lampiran 2 - Borang Permohonan Multimedia ICT
Lampiran 3 - Senarai Perundangan dan Peraturan

PERKARA 1

PEMBANGUNAN DAN PENYELENGGARAAN POLISI

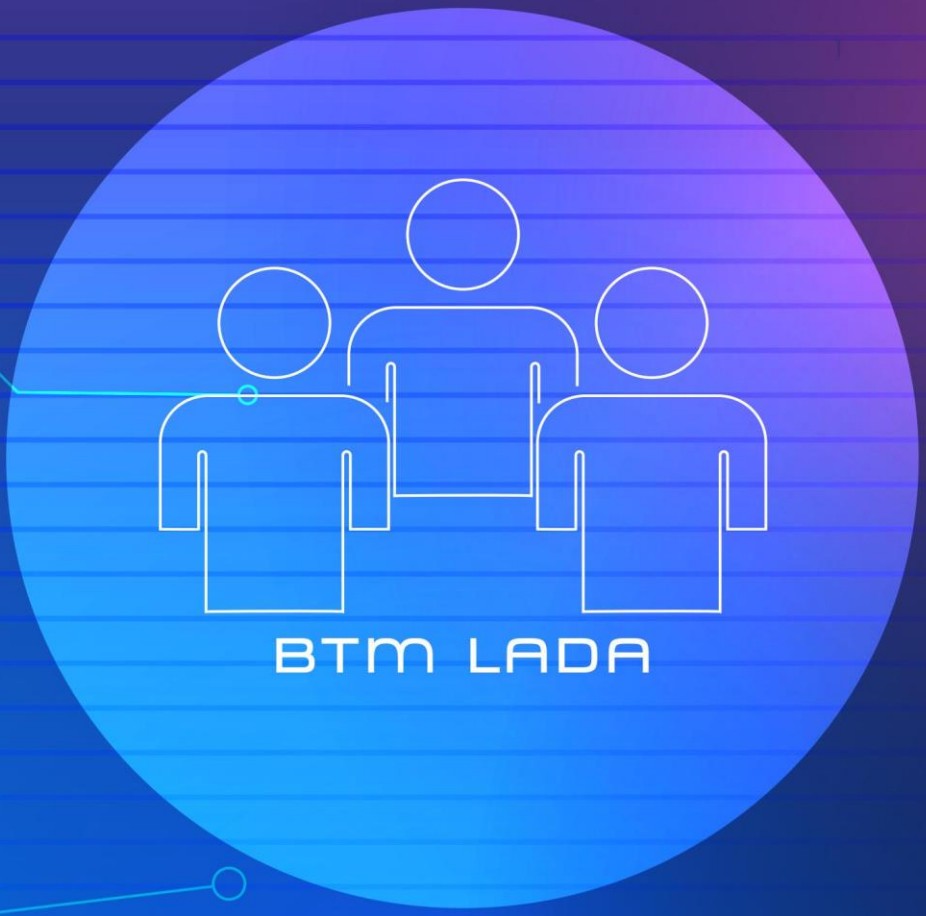
PERKARA 1: PEMBANGUNAN DAN PENYELENGGARAAN POLISI

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
1.1 Polisi ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap pengurusan ICT dan keselamatan maklumat selaras dengan keperluan LADA dan perundangan yang berkaitan**.**	
1.1.1 Pelaksanaan Polisi	
Pelaksanaan polisi ini akan dijalankan oleh TKPE (P) selaku Pengerusi JPICT LADA dan CDO LADA.	TKPE (P)
1.1.2 Penyebaran Polisi	
PKS LADA ini perlu disebarkan kepada semua pengguna dan pihak ketiga yang menggunakan aset ICT LADA.	Pengurus IT
1.1.3 Penyelenggaraan Polisi	
PKS LADA adalah tertakluk kepada semakan dan pindaan daripada semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur penyelenggaraan PKS LADA: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemukakan cadangan pindaan secara bertulis kepada CDO LADA untuk pembentangan dan persetujuan Mesyuarat JPICT LADA; (c) Maklumkan kepada semua pengguna perubahan yang telah dipersetujui oleh JPICT LADA; dan (d) PKS LADA hendaklah dikaji semula mengikut keperluan semasa.	Pengurus IT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
1.1.4 Pengecualian	
PKS LADA adalah terpakai kepada semua pengguna dan pihak ketiga yang menggunakan aset dan perkhidmatan ICT LADA dan tiada pengecualian diberikan.	Semua

PERKARA 2

ORGANISASI ICT



PERKARA 2: ORGANISASI ICT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
2.1 Infrastruktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS LADA.	
2.1.1 Ketua Pegawai Eksekutif (KPE)	
Peranan dan tanggungjawab KPE adalah seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah PKS LADA; (b) Memastikan semua pengguna mematuhi PKS LADA; (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 PKS LADA.	KPE
2.1.2 Ketua Pegawai Digital (CDO)	
Ketua Pegawai Digital (CDO) bagi LADA ialah Timbalan Ketua Pegawai Eksekutif (Pengurusan) LADA. CDO bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di LADA.Peranan dan tanggungjawab CDO adalah seperti berikut: (a) Memantau pelaksanaan Pelan Strategik Pendigitalan LADA yang mengandungi perancangan penggunaan IT dalam menyokong pencapaian matlamat agensi; (b) Memperkenalkan dan menyepadukan proses-proses yang *cross functional* antara Bahagian dan Unit bagi menghasilkan perkhidmatan yang lebih cekap dan berkesan;	CDO

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(c) Menyelaras pembangunan, pengendalian dan pengurusan sistem dan infrastruktur IT yang utuh dan selamat; (d) Menentukan hala tuju sistem aplikasi LADA bagi mengurangkan masa dan kos pembangunan, penyelenggaraan dan pengoperasian; (e) Memelihara integriti data elektronik, menggalak perkongsian maklumat dan menyediakan kaedah bagi penyebaran maklumat secara elektronik kepada pengguna-pengguna yang sah sama ada dalam atau luar LADA; (f) Mempengerusikan Jawatankuasa Pemandu ICT LADA; (g) Mempromosikan kegunaan IT yang berkesan dan seiringan untuk mencapai matlamat strategik LADA dan bertindak sebagai agen dan perintis perubahan (*Champion of Change*); dan (h) Memimpin dan melibatkan LADA dalam usaha-usaha Kerajaan untuk membangun dan melaksanakan projek IT sektor awam yang membawa dalam pengurusan dan pentadbiran Perkhidmatan Awam.	
2.1.3 Pengurus IT	
Peranan dan tanggungjawab Pengurus IT adalah seperti berikut: (a) Merangka, merumus dan menguatkuasakan PKS LADA; (b) Menentukan semua pengguna mendapat pendedahan, bantuan dan mematuhi PKS LADA; (c) Menetapkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan; (d) Menentukan kawalan akses semua pengguna terhadap aset ICT LADA;	Pengurus IT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(e) Memastikan kawalan capaian ke atas aset ICT termasuk maklumat, perkhidmatan rangkaian dan kemudahankemudahan yang berkaitan diwujudkan dan dilaksanakan dengan berkesan berasaskan keperluan urusan dan keselamatan; (f) Mengkaji semula dan memperhalus pengurusan kerahsiaan maklumat dan kawalan capaian secara berkala; (g) Memastikan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT LADA disimpan; dan (h) Merangka, membangun dan merumus *Disaster Recovery Plan* (DRP) yang menyeluruh untuk menjamin perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
2.1.4 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT LADA; (b) Menguatkuasakan perihal keselamatan ICT LADA; (c) Memberi penerangan dan pendedahan berkenaan keselamatan ICT kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan keselamatan ICT di LADA; (e) Menjalankan pengurusan risiko; (f) Menjalankan audit keselamatan, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (g) Memberi amaran terhadap kemungkinan berlakunya	ICTSO

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Sektor Awam (GCERT NACSA MKN) dan memaklumkannya kepada CIO; (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; (j) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar PKS LADA; (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 supaya insiden baharu dapat dielakkan.	
2.1.5 Jawatankuasa Pemandu ICT (JPICT) LADA	
Keahlian JPICT LADA adalah terdiri daripada: (a) Pengerusi (KPE LADA atau Pegawai yang diturunkan kuasa); (b) CDO; (c) Ketua-ketua Bahagian dan Unit di LADA; (d) Pengurus ICT; (e) ICTSO; (f) Ahli-ahli jemputan yang berkaitan; dan (g) BTM sebagai Urus Setia Peranan dan tanggungjawab JPICT LADA adalah seperti berikut: (a) Menetapkan arah tuju dan strategi untuk pelaksanaan ICT LADA;	JPICT LADA

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT LADA; (c) Merancang dan menyelaras pelaksanaan program/projek-projek ICT LADA supaya selaras dengan Pelan Strategik Pendigitalan LADA; (d) Menyelaras dan menyeragamkan pelaksanaan ICT di LADA dengan Pelan Strategik Pendigitalan Sektor Awam dan Pelan Strategik Pendigitalan LADA; (e) Mempromosi dan menggalakkan perkongsian pintar projek ICT antara Kementerian dan semua agensi di bawahnya; (f) Merancang dan menentukan langkah-langkah keselamatan ICT; (g) Mengikuti dan memantau perkembangan program ICT LADA serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT; (h) Menilai dan meluluskan semua perolehan ICT LADA berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan; (i) Mengemukakan laporan kemajuan projek ICT bagi LADA yang telah diluluskan oleh JPICT kepada Kementerian Kewangan mengikut tempoh-tempoh yang telah ditetapkan.	
2.1.6 Pentadbir Sistem ICT	
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Memantau ketersediaan dan prestasi *server*;	Pentadbir Sistem ICT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Menyimpan dan menganalisa rekod jejak audit; (c) Mengambil tindakan pengukuhan bagi meningkatkan tahap keselamatan *server*; (d) Melaksanakan pengemaskinian *patches* Sistem Pengoperasian (OS); (e) Melaksanakan penyelenggaraan pencegahan (*preventive maintenance*) mengikut jadual yang ditetapkan dan penyelenggaraan pembaikan (*corrective maintenance*); (f) Melaksanakan amalan terbaik dalam menjaga keselamatan maklumat terperingkat di bawah kawalan masing-masing daripada pencerobohan dalaman atau luaran, seperti sentiasa melakukan penduaan (*backup*) ke atas data-data penting mengikut jadual yang ditetapkan; dan (g) Mengendalikan penduaan maklumat, sistem, sistem pengoperasian dan data pada *server* dan disimpan di luar kawasan (*off site*) secara berkala.	
2.1.7 Pentadbir Pusat Data	
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: (a) Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; (b) Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; (c) Menjadual dan melaksanakan proses backup dan *restoration* ke atas pangkalan data dan sistem secara berkala; (d) Menyediakan perancangan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan (PKP) dan Pelan Pemulihan Bencana ICT (DRP);	Pentadbir Pusat Data

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(e) Melaksanakan prinsip-prinsip PKS LADA; (f) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan; (g) Melaporkan sebarang pelanggaran keselamatan Pusat Data LADA kepada ICTSO; dan (h) Memastikan maklumat perhubungan perlu dikemaskini dari semasa ke semasa.	
2.1.8 Pentadbir Rangkaian	
Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: (a) Merancang dan mereka bentuk penggunaan dan perkhidmatan rangkaian LAN dan WAN; (b) Memastikan pengguna mendapat segala kemudahan rangkaian termasuk kemudahan Internet serta mengawal dan memantau sistem rangkaian bagi memastikan ia beroperasi ke tahap yang paling berkesan; (c) Bertanggungjawab mengurus dan mengendalikan segala jenis gangguan berkaitan perkhidmatan rangkaian; (d) Mengurus perkhidmatan pengalamatan *Internet Protocol* (IP) menggunakan *Dynamic Host Configuration Protocol* (DHCP) dan statik bagi server serta *Domain Controller* LADA; (e) Mengendalikan urusan permohonan *public* IP, pembukaan port serta pendaftaran *Domain Name Server* (DNS) dalaman dan luaran bagi server dan sistem aplikasi yang memerlukan; (f) Mengenal pasti dan mengkaji keperluan perlaksanaan dan peningkatan kawalan keselamatan ke atas rangkaian; (g) Menyelenggara semua peralatan-peralatan rangkaian yang terdapat di LADA serta mengemaskini inventori peralatan-peralatan rangkaian tersebut;	Pentadbir Rangkaian

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(h) Mengendalikan urusan perolehan peralatan rangkaian termasuk menyediakan kertas kerja berkaitan dengannya; dan (i) Memberi bantuan teknikal rangkaian kepada semua pengguna rangkaian di LADA;	
2.1.9 Pentadbir Pangkalan Data	
Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: (a) Menjalankan tugas pentadbir pangkalan data dengan memastikan semua pangkalan data yang dibangunkan diurus secara optima dan bertanggungjawab terhadap integriti data dan penggunaan pangkalan data; (b) Bertanggungjawab terhadap pengoperasian harian pangkalan data termasuklah membaiki prestasi, *recovery*, *tuning* dan lain-lain; (c) Bertanggungjawab untuk menganalisa dan menyemak log pangkalan data melalui perisian penganalisa log yang diperolehi bagi tujuan menganalisa *behavior* setiap pangkalan data yang berkaitan ; dan (d) Mengendalikan urusan perolehan perkakasan dan perisian komputer termasuk penyediaan kertas kerja berkaitan.	Pentadbir Pangkalan Data
2.1.10 Pentadbir Sistem Aplikasi	
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti 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 PKS LADA;	Pentadbir Sistem Aplikasi

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(c) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (d) Melaporkan aktiviti-aktiviti tidak normal kepada ICTSO dengan segera; dan (e) Menyediakan laporan mengenai aktiviti capaian yang mencurigakan kepada pemilik maklumat sekiranya perlu.	
2.1.11 Koordinator ICT Bahagian	
Setiap bahagian di LADA akan melantik Koordinator ICT masing-masing. Peranan dan tanggungjawab Koordinator ICT adalah seperti berikut: (a) Pegawai perhubungan (*liaison officer*) bahagian bagi perkara berkaitan kemudahan ICT; i. Keperluan perkakasan dan perisian ICT • Mengenal pasti keperluan bahagian dan mengemukakan permohonan kepada BTM; dan • Mengemukakan isu-isu berkaitan ICT kepada BTM. ii. Pemulangan aset ICT yang tidak digunakan • Memaklumkan kepada BTM nama pegawai yang akan bertukar dan menyelaras pemulangan aset kepada BTM. iii. Kehilangan perkakasan ICT • Memaklumkan sebarang kehilangan perkakasan dan perisian ICT kepada BTM serta melaporkan kehilangan tersebut kepada Pegawai Aset LADA. iv. Penyelenggaraan Pencegahan (PM) Perkakasan ICT • Memaklumkan kepada semua pegawai di bahagian masing-masing tentang aktiviti penyelenggaraan pencegahan yang akan dilakukan oleh BTM; dan • Memastikan semua bilik/ruang kerja pegawai	Koordinator ICT Bahagian

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
dapat diakses oleh wakil BTM semasa aktiviti penyelenggaraan pencegahan dilakukan. v. Pelupusan aset ICT • Memaklumkan kepada BTM aset ICT yang rosak dan perlu dilupuskan; dan • Mengumpulkan aset ICT tersebut dan menghantar ke BTM. vi. Menyelaras keperluan latihan ICT bahagian; vii. Memaklumkan kepada BTM pegawai baharu yang perlu menandatangani Surat Akuan Pematuhan PKS LADA;dan viii. Wakil bahagian dalam Mesyuarat Koordinator ICT yang diadakan oleh BTM.	
2.1.12 Koordinator Web Bahagian	
Setiap bahagian di LADA akan melantik Koordinator Web masing-masing. Peranan dan tanggungjawab Koordinator Web Bahagian adalah seperti berikut: (a) Memaklumkan mengenai maklumat perkhidmatan yang dikendalikan oleh bahagian; (b) Menyumbang maklumat dalam menambahbaik kandungan laman web LADA; (c) Menyemak soalan lazim bahagian; dan (d) Menyemak dan memastikan maklumat bahagian dikemas kini.	Koordinator Web Bahagian
2.1.13 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: (a) Membaca, memahami dan mematuhi PKS LADA;	Pengguna

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Lulus tapisan keselamatan atau yang setaraf dengannya; (c) Melaksanakan prinsip-prinsip PKS LADA dan menjaga kerahsiaan maklumat LADA; (d) Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Menjaga kerahsiaan kata laluan; iii. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; iv. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; v. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; vi. Menandatangani Surat Akuan Pematuhan PKS LADA sebagaimana Lampiran 1; dan vii. Melaksanakan amalan terbaik dalam menjaga keselamatan maklumat terperingkat di bawah kawalan masing-masing dari pencerobohan dalaman atau luaran seperti: • Melakukan penyulitan (*encryption*) ke atas maklumat terperingkat; • *Lock* komputer desktop (PC) apabila tiada di tempat; dan • Menutup PC sebelum balik atau selepas waktu pejabat.	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
2.2 Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.	
2.2.1 Pembekal, Kontraktor, Pakar Runding, Pelawat dan Pihak-Pihak Luar Lain	
Peranan dan tanggungjawab pihak luar/asing adalah seperti berikut: (a) Membaca, memahami dan mematuhi PKS LADA di mana berkenaan; (b) Bertanggungjawab ke atas sebarang perlanggaran keselamatan disebabkan tindakannya sendiri; (c) Melaporkan insiden keselamatan ICT dengan kadar segera kepada ICTSO; (d) Menjaga kerahsiaan data dan maklumat LADA; (e) Menandatangani Surat Akuan Pematuhan PKS LADA sebagaimana Lampiran 1; (f) Menandatangani Borang Akta Rahsia Rasmi yang boleh diperoleh daripada Bahagian Sumber Manusia dan Khidmat Pengurusan; dan (g) Lulus tapisan keselamatan atau yang setaraf dengannya.	Pihak Ketiga

PERKARA 3

PENGURUSAN ASET

PERKARA 3: PENGURUSAN ASET

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
3.1 Perolehan Aset ICT	
Objektif: Memastikan perolehan Aset ICT mengikut prosedur yang telah ditetapkan	
3.1.1 Perolehan Perkakasan, Perisian dan Perkhidmatan ICT	
Perkara yang perlu dipatuhi adalah seperti berikut:	
(a) Tatacara perolehan perkakasan, perisian dan perkhidmatan ICT hendaklah merujuk kepada pekeliling terpakai sedia ada;	Semua
(b) Setiap bahagian di LADA perlu mengemukakan permohonan perolehan projek ICT kepada BTM untuk tujuan penyelarasan sebelum memohon kelulusan teknikal JPICT LADA/JPICT MOF/JTISA (berdasarkan kos projek) dan semua perolehan ICT hendaklah mendapat kelulusan peruntukan terlebih dahulu;	Semua bahagian dan BTM
(c) Skop projek ICT yang memerlukan kelulusan teknikal JPICT LADA adalah merujuk kepada Garis Panduan Pelaksanaan Projek Teknologi Maklumat dan Komunikasi LADA. Secara asasnya, semua projek ICT yang melibatkan pembangunan, naiktaraf, perluasan, pertambahan dan penyelenggaraan sistem aplikasi, laman web, perkakasan, perisian, rangkaian dan perkhidmatan ICT adalah memerlukan kelulusan teknikal ICT.	Semua
(d) Skop projek yang DIKECUALIKAN kelulusan teknikal JPICT LADA juga adalah merujuk kepada kepada Garis Panduan Pelaksanaan Projek Teknologi Maklumat dan Komunikasi LADA. Secara asasnya, komponen alat ganti, barang pakai habis (consumable item), aksesori, perabot komputer, kamera, projektor, CCTV, penyaman udara, telefon pintar (smartphone) dan seumpamanya tidak memerlukan kelulusan teknikal JPICT LADA.	Semua
	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(e) Had nilai dan peringkat kelulusan teknikal projek ICT adalah seperti yang dinyatakan dalam Garis Panduan Pelaksanaan Projek Teknologi Maklumat dan Komunikasi LADA.	
3.2 Peruntukan / Perkongsian Perkakasan dan Perisian ICT	
Objektif: Memastikan perkakasan dan perisian ICT diagihkan mengikut kelayakan dan keperluan.	
3.2.1 Komputer Desktop (PC), Komputer Riba dan Peralatan Guna Sama	
Perkara yang perlu dipatuhi adalah seperti berikut:	
(a) Setiap pegawai layak diperuntukkan satu (1) unit komputer *desktop*/komputer riba mengikut keperluan dan jenis yang sesuai: i. Kumpulan Pengurusan Tertinggi dibekalkan dengan komputer *desktop*; ii. Kumpulan Pengurusan dan Profesional (P&P) diberi pilihan untuk dibekalkan dengan komputer *desktop* atau komputer riba; iii. Kumpulan Pengurusan dan Profesional (P&P) berstatus kontrak dibekalkan dengan komputer *desktop*; iv. Kumpulan Pelaksana dibekalkan dengan komputer *desktop* mengikut norma kerja; dan v. Setiap bahagian akan diperuntukkan dengan satu unit komputer riba untuk kegunaan guna sama di bahagian.	BTM
(b) Setiap komputer *desktop* dan komputer riba dilengkapkan dengan perisian asas seperti sistem pengoperasian, perisian *desktop productivity*, pelayar web, *antivirus* dan perisian *remote* akses untuk tujuan pentadbiran dan penyelenggaraan. Perisian yang dipasang perlu mempunyai lesen yang sah.	Semua BTM
(c) Auditorium, Dewan Besar dan semua bilik mesyuarat utama disediakan dengan kemudahan komputer *desktop*.	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(d) Perkara di 3.2.1.a adalah tertakluk kepada ketersediaan perkakasan sedia ada.	BTM
3.2.2 Pencetak	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengurusan Tertinggi dan Pengurus Bahagian diperuntukkan dengan sebuah pencetak *monochrome light duty*. (b) Kumpulan Pengurusan dan Profesional (P&P) berstatus tetap dan kontrak berkelayakan untuk dibekalkan dengan pencetak *monochrome light duty* berdasarkan keperluan; (c) Kumpulan Pelaksana dibekalkan dengan pencetak guna sama; (d) Setiap bahagian di LADA diperuntukkan pencetak guna sama yang dipusatkan untuk kegunaan semua pegawai dan kakitangan; (e) Selain perkara 3.2.2.(a) sehingga perkara 3.2.2.(d), pencetak jenis *monochrome light duty* akan dibekalkan dan diguna secara guna sama dengan nisbah yang difikirkan sesuai untuk kelancaran kerja dan jenis kerja yang dilakukan seperti kerahsiaan maklumat, kedudukan tempat dan proses kerja.	BTM
3.2.3 Peralatan Sidang Video	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap bilik mesyuarat utama diperuntukkan peralatan sidang video.	BTM

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
3.3 Akauntabiliti Aset	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT LADA.	
3.3.1 Inventori Aset	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua aset ICT LADA hendaklah direkodkan dalam Sistem Pengurusan Aset (SPA). Ini termasuklah merekodkan maklumat penempatan dan penyelenggaraan sehingga pelupusan aset berkenaan. (b) Setiap aset ICT diagihkan kepada pengguna mengikut piawaian dan garis panduan yang ditetapkan. (c) Aset ICT perlu mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. (d) Peraturan bagi pengendalian aset ICT hendaklah dipatuhi dan dilaksanakan; (e) Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah kawalannya.	BTM/Pegawai Aset Bahagian Semua
3.3.2 Peralatan Sewaan	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Perkhidmatan sewaan peralatan ICT perlu merangkumi kerja-kerja membekal, menghantar, memasang, mengkonfigurasi, menguji, mentauliah dan menyelenggara peralatan ICT; (b) Peralatan ICT yang disewa mestilah produk semasa, baru, tulen dan belum pernah digunakan; (c) Kerja-kerja penyelenggaraan peralatan ICT sewaan adalah kerja-kerja pembaikan kerosakan, penggantian	Semua

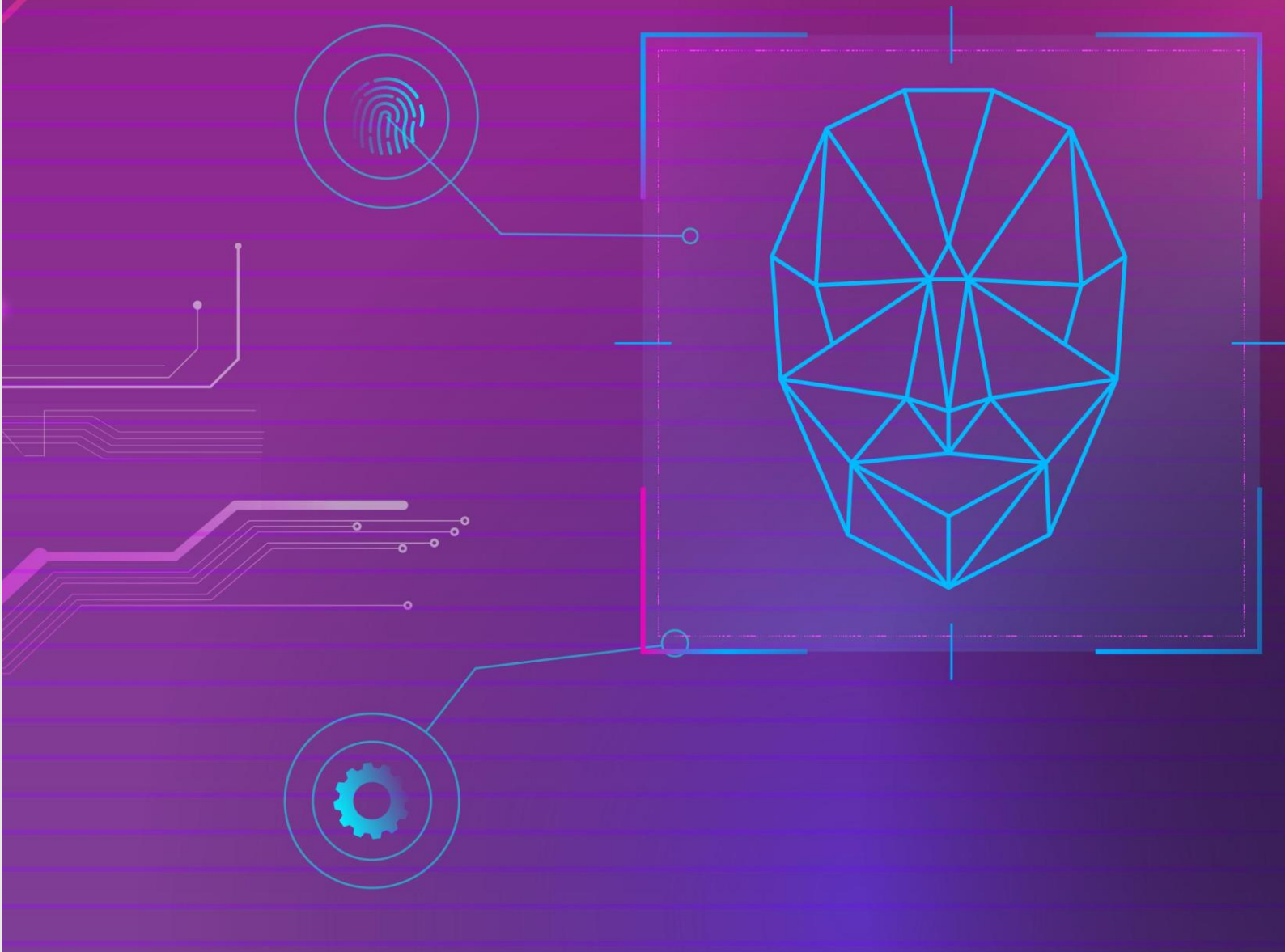
PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
mana-mana bahagian atau alat ganti yang rosak dan penyelenggaraan pencegahan yang dijadualkan mengikut kesesuaian peralatan tersebut; (d) Kakitangan yang menerima peralatan sewaan perlu menjaga dan memastikan peralatan yang diterima sentiasa dalam milik LADA, tidak memindahkan kepada hak milik lain, berkeadaan baik dan tidak rosak akibat kecuaian kakitangan; (e) Kesemua data yang disimpan di dalam peralatan yang disewa perlu dipadamkan sebelum peralatan diserahkan kembali kepada pembekal selepas tamat tempoh sewaan; dan (f) Waranti peralatan ICT yang disewa adalah waranti dari prinsipal peralatan.	
3.4 Pengelasan dan Pengendalian Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
3.4.1 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
3.4.2 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menjaga kerahsiaan kata laluan; (d) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (e) Meletakkan kawalan seperti katalaluan bagi maklumat terperingkat sebelum melakukan transmisi; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	Semua
3.4.3 Keselamatan Maklumat	
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Maklumat terperingkat hanya boleh dilakukan penduaan dan penyalinan pada media storan oleh pegawai yang dibenarkan sahaja; (b) Menggunakan enkripsi dan lain-lain kaedah keselamatan yang bersesuaian ke atas maklumat terperingkat yang disediakan dan dihantar secara elektronik; dan	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(c) Semua maklumat terperingkat hendaklah dihapuskan mengikut prosedur pelupusan semasa.	
3.5 ICT Hijau (Green ICT)	
Objektif: Memastikan aset ICT mempunyai ciri-ciri ICT Hijau.	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan perolehan aset ICT mempunyai spesifikasi ciri-ciri ICT Hijau; (b) Memastikan kerja-kerja seharian mengguna pakai prinsip pengurangan (*reduce*), penggunaan semula (*reuse*) dan kitar semula (*recycle*); (c) Memastikan sistem pengurusan kuasa (power *management*) aset ICT diaktifkan; dan (d) Memastikan peralatan ICT dilupuskan dan penggunaan semula alat ganti mengikut tatacara yang mengambil kira pemuliharaan alam sekitar.	BTM dan Pengguna

PERKARA 4

KESELAMATAN SUMBER MANUSIA



PERKARA 4: KESELAMATAN SUMBER MANUSIA

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
4.1 Keselamatan Manusia Dalam Tugas Harian	
Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan LADA, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga LADA hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
4.1.1 Sebelum Memulakan Perkhidmatan	
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan LADA serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan LADA 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
4.1.2 Dalam Perkhidmatan	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan pegawai dan kakitangan LADA serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh LADA;	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT LADA secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan LADA serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh LADA; 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.	
4.1.3 Bertukar atau Tamat Perkhidmatan	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikembalikan kepada LADA mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (b) Memulangkan dan menghapuskan sebarang dokumen atau maklumat rasmi yang berkaitan dengan tugas atau tempat di mana ia ditugaskan; dan (c) Membatalkan atau menghapuskan semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh LADA dan/atau terma perkhidmatan selepas 3 hari bekerja.	BTM dan Semua

PERKARA 5

KESELAMATAN FIZIKAL DAN PERSEKITARAN

PERKARA 5: KESELAMATAN FIZIKAL DAN PERSEKITARAN

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
5.1 Keselamatan Kawasan	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
5.1.1 Kawalan Kawasan	
Bertujuan menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan dan lain-lain) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Melindungi kawasan terhad melalui kawalan-kawalan tertentu seperti memasang alat penggera atau kamera litar tertutup sekiranya berkaitan; (d) Mengehadkan jalan keluar masuk; (e) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (f) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan yang disediakan; dan (g) Memastikan kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	Pegawai Keselamatan Jabatan

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
5.1.2 Kawasan Larangan	
Kawasan Larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Pusat Data adalah Kawasan Larangan, di mana: (a) Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; (b) Pusat Data LADA terbahagi kepada 3 ruang utama iaitu *staging*, *command center* dan bilik server; (c) Tanda Kawasan Larangan hendaklah dipamerkan; (d) Buku Log Keluar/Masuk Pusat Data disediakan dan disemak secara berjadual; (e) Pihak ketiga adalah dibenarkan memasuki Pusat Data bagi memberi perkhidmatan sokongan atau bantuan teknikal. Walau bagaimanapun, mereka hendaklah diiringi sepanjang masa sehingga tugas selesai; (f) Semua aktiviti dan penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat hendaklah dikawal dan mendapat kebenaran daripada Pengurus IT/ Pentadbir Pusat Data; (g) Peralatan rakaman/penyimpanan seperti kamera, video, perakam suara dan storan mudah alih adalah tidak dibenarkan dibawa masuk ke dalam Pusat Data kecuali dengan kebenaran Pengurus IT/ Pentadbir Pusat Data; (h) Pusat Data perlu dilengkapi dengan kawalan perlindungan keselamatan fizikal seperti penghawa dingin khas, *Uninteruptable Power Supply, Water Leak Detection System, Fire Suppression System, High Sensitivity Smoke Detection System, Environment Monitoring System,* kawalan pintu masuk, alat penggera dan kamera litar tertutup;	Pentadbir Pusat Data

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(i) Suhu Pusat Data perlu ditetapkan di antara 19°C hingga 24°C dengan kelembapan pada tahap 60% hingga 70%; (j) Laluan yang menghubungkan Pusat Data dengan ruang-ruang atau bilik-bilik lain seperti ruang penyimpanan dan kawasan luar bangunan tidak boleh mempunyai sebarang halangan; (k) Semua perabot kecuali kerusi di dalam Pusat Data adalah diperbuat daripada logam atau besi; (l) Barang-barang yang tidak digunakan tidak boleh ditinggalkan dan dilarang membawa masuk makanan ke dalam Pusat Data. Contohnya: kotak peralatan, bahan api yang mudah terbakar, plastik makanan, cawan kertas dan sebagainya; (m) Pusat Data adalah kawasan larangan merokok; (n) Kapasiti UPS Pusat Data boleh menampung maksimum tiga (3) jam sekiranya bekalan kuasa elektrik terputus; (o) Semua peralatan dalam Pusat Data perlu dilabelkan bagi memudahkan setiap pentadbir menjalankan tugas masing-masing; (p) Diagram kedudukan *server* disediakan dan dipamerkan dalam Pusat Data dan perlu dikemaskini; (q) Memaparkan maklumat pegawai dan organisasi yang boleh dihubungi sekiranya berlaku kecemasan; (r) Memastikan semua permohonan penempatan, peralihan dan pengeluaran sebarang peralatan dalam Pusat Data mendapat kelulusan Pengurus IT/Pentadbir Pusat Data; (s) Memastikan semua pintu sentiasa ditutup dan Sistem Pintu Keselamatan berfungsi dengan baik; (t) Melaksanakan kesinambungan perkhidmatan Pusat Data termasuk pemulihan Pusat Data sekiranya berlaku bencana; dan	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(u) Memastikan Pusat Data disenggara mengikut jadual yang telah ditetapkan berdasarkan kesesuaian peralatan dan disahkan oleh Pengurus ICT/Pentadbir Pusat Data.	
5.1.3 Kawasan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Pas keselamatan hendaklah dipakai sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan semula kepada LADA apabila pengguna berpindah keluar, berhenti atau bersara. Pihak ketiga juga hendaklah berbuat demikian apabila urusan selesai atau tamat kontrak; (c) Pas pelawat hendaklah diambil di kaunter masuk. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan segera.	Pengguna dan Pihak Ketiga
5.2 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT LADA daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
5.2.1 Peralatan ICT	
Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna. Sebarang kerosakan peralatan ICT hendaklah dilaporkan melalui saluran yang ditetapkan;	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran dan perubahan konfigurasi yang telah ditetapkan; (c) Dilarang sama sekali menambah, mengganti atau mengeluarkan sebarang perkakasan ICT yang telah ditetapkan; (d) Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran; (e) Bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) Memastikan perisian antivirus yang dibekalkan oleh LADA di komputer peribadi/komputer riba sentiasa aktif (activated) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; (g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan dan diperbaharui mengikut tempoh yang ditetapkan; (h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (i) Peralatan-peralatan kritikal perlu disokong oleh UPS; (j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (l) Peralatan ICT yang hendak dibawa keluar dari premis LADA hendaklah mematuhi peraturan yang telah ditetapkan;	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(m) Peralatan ICT yang hilang hendaklah dilaporkan kepada Pengurus ICT dan Pegawai Aset LADA/Bahagian/Unit dengan segera; (n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (o) Pengguna tidak dibenarkan mengubah kedudukan peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran BTM/Pegawai Aset LADA/Bahagian/Unit. Perpindahan peralatan ICT hendaklah mematuhi peraturan yang telah ditetapkan; (p) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (q) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (r) Bertanggungjawab terhadap peralatan ICT di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (s) Memastikan semua peralatan ICT yang tidak digunakan dalam keadaan tutup (*off*) apabila meninggalkan pejabat; (t) Memastikan *plug* dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat; dan (u) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pengurus IT dan tindakan penarikan balik kemudahan boleh diambil.	
5.2.2 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, pita magnetik, *optical disk, flash disk*, CD/DVD ROM, *thumb drive, external hard disk* dan media storan lain.	BTM dan Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
Media/perkhidmatan 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 sesuai dan mempunyai ciri-ciri keselamatan berpadanan dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; (c) Akses dan pergerakan media storan hendaklah direkodkan; (d) Kehilangan media storan yang berlaku hendaklah dilaporkan mengikut peraturan semasa yang ditetapkan; (e) Sebarang aktiviti penghapusan maklumat yang terkandung dalam media/perkhidmatan storan, mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; (f) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; dan (g) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat mengikut prosedur pelupusan.	
5.2.3 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;	Pengguna

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(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.	
5.2.4 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perisian-perisian ICT yang disokong oleh BTM untuk pemasangan, penyelenggaraan dan latihan adalah termasuk: i) MS Office yang terdiri daripada: • MS Word • MS Excel • MS Powerpoint • MS Project ii) Web Browser iii) Acrobat Reader iv) WinZip v) Antivirus vi) Adobe Creative Cloud vii) AutoCAD viii) Perisian *video conferencing* LADA ix) Anydesk (b) Sokongan untuk perisian yang tidak tersenarai di item (a) hanya akan diberikan sekiranya ada tenaga kepakaran di BTM; (c) Hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa boleh dipasang dan digunakan; (d) BTM boleh mengesan dan berhak membuang (*uninstall*) perisian yang tidak diperakui tanpa perlu mendapat kebenaran pengguna;	BTM dan Pengguna

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(e) Pengguna tidak dibenarkan membuang sebarang perisian yang telah dipasang oleh BTM di dalam komputer *desktop* atau komputer riba masing-masing; (f) Pengguna mesti memastikan media storan yang menyimpan dokumen terperingkat disimpan di tempat yang selamat; dan (g) Pengguna mesti memastikan maklumat rahsia rasmi yang terkandung dalam media storan dikawal dan dilindungi dengan perisian penyulitan (*encryption*) yang disyorkan oleh BTM.	
5.2.5 Penyelenggaraan Perkakasan	
Proses kerja penyelenggaraan peralatan ICT adalah merujuk kepada Prosedur Penyelenggaraan ICT LADA (ISO). Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan oleh pengeluar; (b) Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Semua perkakasan hendaklah disemak serta diuji sebelum dan selepas proses penyelenggaraan (*Preventive Maintenance*) dilakukan; (d) Penyelenggaraan Pencegahan dilaksanakan mengikut jadual kekerapan yang telah ditetapkan berdasarkan jenis perkakasan; (e) Penyelenggaraan peralatan perkakasan ICT di bahagian-bahagian perlulah diselaras oleh BTM bagi memudahkan pemantauan dan inventori;	Pengguna, Pegawai Aset dan BTM

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(f) Pengurusan katalaluan *administrator* bagi setiap komputer/laptop di LADA adalah dibawah pengendalian BTM LADA. (g) Setiap pengguna di lokasi penyelenggaraan perlu mengesahkan kerja-kerja penyelenggaraan yang dilakukan. (h) Proses *backup* perlu dilaksanakan sendiri oleh pengguna. Namun begitu, pengguna boleh mendapatkan khidmat nasihat dan bantuan teknikal daripada BTM; (i) Perisian sistem pengoperasian bagi perkakasan ICT di LADA, dikonfigurasi supaya dikemas kini *patches* dan dinaiktarafkan (*upgrades*) kepada versi terkini secara automatik; dan (j) Bantuan teknikal/aduan tentang masalah-masalah yang dihadapi dalam penggunaan ICT perlu diajukan kepada BTM.	
5.2.6 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis LADA adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan bahagian/Pegawai Aset Bahagian/pegawai yang diberi kuasa dan tertakluk kepada tujuan yang dibenarkan; (b) Bagi peralatan guna sama yang dipinjam, aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan; (c) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (d) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pengguna, Pegawai Aset Bahagian dan BTM

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
5.2.7 Pelupusan Peralatan ICT	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak ekonomi dibaiki sama ada harta modal atau inventori yang dibekalkan. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan LADA. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT yang hendak dilupuskan perlulah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (b) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT; (c) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; (d) Pengguna adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Contohnya: CPU, RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti UPS, *speaker* dan mana-mana peralatan yang berkaitan ke mana- mana bahagian; iii. Memindah keluar dari lokasi mana-mana peralatan ICT yang hendak dilupuskan (e) Semua kandungan dan maklumat dalam peralatan ICT khususnya maklumat rahsia rasmi hendaklah	Pengguna, Pegawai Aset dan BTM

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degaussing, electronic data erasure* atau pembakaran; (f) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan (g) Pelupusan adalah tertakluk kepada Pekeliling Perbendaharaan (PP) Pengurusan Aset bertajuk ”Tatacara Pengurusan Aset Alih Kerajaan” atau pekeliling terbaharu yang berkuatkuasa.	
5.2.8 Pindahan Peralatan ICT	
Pindahan melibatkan semua peralatan ICT yang sudah tidak digunakan lagi tetapi masih berkeadaan baik sama ada harta modal atau inventori yang dibekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT yang hendak dipindahkan perlulah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (b) Pegawai Aset bertanggungjawab merekodkan butir-butir pindahan dan mengemas kini rekod pindahan peralatan ICT; (c) Pindahan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pindahan semasa yang berkuat kuasa; dan (d) Pengguna adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dipindahkan untuk milik peribadi. Contohnya: CPU, RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana	Pengguna, Pegawai Aset dan BTM

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
peralatan yang berkaitan ke mana- mana bahagian; dan iii. Memindah keluar dari lokasi mana-mana peralatan ICT yang hendak dipindahkan.	
5.3 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT LADA daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
5.3.1 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, mengubahsuai atau pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: (a) Merancang dan menyediakan pelan keseluruhan susun atur Pusat Data/DRC (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) Semua kawasan larangan khususnya bilik pemprosesan maklumat dan perkakasan ICT yang menyimpan data dan maklumat rahsia rasmi tidak boleh dilabel. Ia perlu dilindungi dari sebarang pendedahan dan akses oleh individu yang tidak dibenarkan;	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(e) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (f) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; (g) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; (h) Semua peralatan perlindungan hendaklah diselenggara secara berkala. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan (i) Memastikan pegawai yang bertanggungjawab menyimpan kunci dapat dihubungi apabila keadaan memerlukan berbuat demikian.	
5.3.2 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*) perlu digunakan bagi perkhidmatan kritikal seperti di Pusat Data LADA supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Pegawai Keselamatan Jabatan dan ICTSO

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
5.3.3 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 mengelakkan ancaman kerosakan dan *wire tapping*; (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; (e) Pemasangan kabel hendaklah mengikut standard dan kod warna yang ditetapkan serta rapi; (f) Sistem pengkabelan kabel elektrik hendaklah dipasang di melalui *trunking* yang berasingan daripada *trunking* yang mengandungi kabel data; dan (g) Jarak yang disyorkan bagi memisahkan kedua-dua jenis kabel tersebut adalah sekurang-kurangnya 0.5 meter. Ini adalah bagi mengelakkan daripada berlakunya *electromagnetic interference* (EMI) yang boleh menganggu transmisi data.	Pentadbir Pusat Data dan Pentadbir Rangkaian
5.3.4 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan yang dilantik.	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
5.4 Keselamatan Dokumen	
Objektif: Melindungi maklumat LADA daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
5.4.1 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Sistem dokumentasi atau penyimpanan maklumat hendaklah dipastikan selamat dan terjamin; (b) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terhad, Sulit, Rahsia atau Rahsia Besar; (c) Pergerakan fail dan dokumen hendaklah dikawal dan direkodkan serta perlulah mengikut prosedur keselamatan; (d) Dokumen yang mengandungi bahan atau maklumat sensitif hendaklah diambil segera dari pencetak; (e) Menggunakan penyulitan (*encryption*) ke atas dokumen sulit dan terhad yang disediakan dan dihantar secara elektronik; (f) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan Kerajaan; (g) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa; dan (h) Penyimpanan maklumat rasmi terperingkat di storan dalam talian umum (Contohnya: Google Drive dan Dropbox) tidak dibenarkan sama sekali.	Semua

PERKARA 6

PENGURUSAN OPERASI DAN KOMUNIKASI

PERKARA 6: PENGURUSAN OPERASI DAN KOMUNIKASI

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
6.1 Pengurusan Prosedur Operasi	
Objektif: Memastikan operasi ICT berfungsi dengan lancar dan efisien serta selamat daripada sebarang ancaman dan gangguan.	
6.1.1 Pengendalian Prosedur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Prosedur pengurusan operasi ICT hendaklah didokumen, dikawal dan diguna pakai; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti turutan aktiviti, peranan dan tanggungjawab, kekerapan dikendalikan dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pengurus ICT, Pentadbir Pusat Data, Pentadbir Sistem ICT, Pentadbir Sistem Aplikasi, Pentadbir Rangkaian
6.1.2 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 aset ICT terlebih dahulu; (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	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
6.1.3 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) Aset ICT yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan daripada aset ICT yang digunakan sebagai persekitaran sebenar (*production*). Pengasingan juga merangkumi tindakan memisahkan antara kumpulan sistem dan operasi.	Pengurus ICT
6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat serta penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
6.2.1 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;	Pengurus IT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Memantau perkhidmatan dan menyemak laporan serta rekod yang dikemukakan oleh pihak ketiga serta melaksanakan audit secara berkala; dan (c) Mengurus sebarang perubahan terhadap pembekalan perkhidmatan dengan mengambil kira tahap kritikal perkhidmatan dan proses yang terlibat serta melaksanakan penilaian semula risiko keselamatan.	
6.3 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
6.3.1 Perancangan Kapasiti	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan (b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pengurus IT, Pentadbir Pusat Data, Pentadbir Sistem ICT, Pentadbir Sistem Aplikasi, Pentadbir Rangkaian
6.3.2 Penerimaan Sistem Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua sistem baharu (termasuklah sistem yang dinaik taraf) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui; (b) Sebarang penyerahan atau penerimaan sistem baharu perlu mendapat pengesahan/kelulusan pemilik sistem dan	Pengurus IT, Pentadbir Sistem Aplikasi dan Pemilik Sistem

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
perlu melalui proses UAT (*User Acceptance Test*) dan FAT (*Final Acceptance Test*); dan (c) Penyelenggaraan sistem tersebut adalah berdasarkan manual operasi dan prosedur yang ditetapkan.	
6.3.3 Penerimaan Perkakasan dan Perisian Sistem Baharu	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan dan perisian sistem baharu (termasuklah pengemaskinian *patches*) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui; (b) Sebarang penyerahan atau penerimaan perkakasan dan perisian sistem perlu mendapat pengesahan/kelulusan pemilik sistem dan perlu melalui proses SAT (*System Acceptance Test*); dan (c) Penyelenggaraan sistem tersebut adalah berdasarkan manual operasi dan prosedur yang ditetapkan.	Pengurus IT, Pentadbir Sistem ICT dan Pemilik Sistem
6.4 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.	
6.4.1 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus dan *Intrusion Detection System* (IDS), *Intrusion Protection System* (IPS) dan mengikut prosedur penggunaan yang betul dan selamat; (b) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;	BTM dan Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(c) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (d) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (e) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (f) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (g) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
6.4.2 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
6.5 *Housekeeping*	
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bilabila masa.	
6.5.1 Penduaan	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat salinan penduaan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terkini; (b) Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi;	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(c) Menguji sistem penduaan sedia ada bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan (d) Kekerapan penduaan bagi sistem dan aplikasi adalah seperti berikut: i. LAMAN WEB Kekerapan : Setiap hari Jenis Backup : *Full Backup* *Retention* : 60 hari ii. MAIL GATEWAY Kekerapan : Setiap Minggu Jenis Backup : *Full Backup* *Retention* : 8 minggu iii. PANGKALAN DATA Kekerapan : Setiap hari Jenis Backup : *Full Backup* *Retention* : 90 hari iv. EMAIL Kekerapan : Setiap hari Jenis Backup : *Incremental Backup* *Retention* : 90 hari v. EMAIL ARCHIVING Kekerapan : Setiap hari Jenis Backup : *Incremental Backup* *Retention* : 7 hari vi. SISTEM KEWANGAN (GRP) – termasuk semua komponen sistem GRP Kekerapan : Setiap hari Jenis Backup : *Incremental Backup* *Retention* : 7 hari	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
6.6 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
6.6.1 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian LADA merujuk kepada skop seperti berikut : (a) Rangkaian setempat dan talian Internet Kompleks dan premis LADA yang diselenggara oleh BTM; dan (b) Talian MyGOVNET LADA 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) Semua komunikasi rangkaian dari LADA ke sistem luar hendaklah melalui rangkaian berpusat LADA untuk memudahkan pengurusan, penguatkuasaan dan pemantauan terhadap sebarang ancaman keselamatan ICT; (b) Pengasingan antara kerja-kerja pengoperasian rangkaian dan pengkomputeran perlu dilaksanakan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (c) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas daripada risiko seperti banjir, gegaran dan habuk; (d) Rak peralatan rangkaian hanya menempatkan peralatan rangkaian sahaja; (e) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (f) Peralatan rangkaian harus diselenggara secara berkala oleh kakitangan atau pihak yang dibenarkan sahaja;	Pentadbir Pusat Data dan Pentadbir Rangkaian

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(g) Peralatan rangkaian yang kritikal harus mempunyai kontrak penyelenggaraan yang menyeluruh dan berkala; (h) Semua peralatan mestilah melalui proses ujian penerimaan selepas pemasangan dan konfigurasi; (i) Semua jenis perisian *sniffer* atau *network analyzer* adalah dilarang dipasang kecuali mendapat kebenaran ICTSO; (j) Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat LADA; (k) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan"; (l) Urusan pendaftaran domain LADA hanya dilakukan oleh BTM sahaja; (m) Pelawat dan pengguna luar hanya dibenarkan untuk menggunakan capaian internet tanpa wayar yang dikhaskan untuk pelawat; (n) Sebarang penyambungan rangkaian yang bukan di bawah kawalan LADA hendaklah mendapat kebenaran ICTSO; dan (o) Semua pengguna hanya dibenarkan menggunakan rangkaian LADA sahaja.	
6.6.2 Sambungan Rangkaian	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna tidak dibenarkan sama sekali memasang sebarang *access point* untuk capaian secara tanpa wayar (*wireless*) dalam rangkaian LADA;	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Pengguna tidak dibenarkan memutuskan/menyambung sambungan kabel UTP pada mana-mana port dalam rak peralatan rangkaian; (c) Perbuatan yang boleh merosakkan UTP port, kabel UTP atau rak peralatan rangkaian serta peralatannya adalah dilarang; (d) Pengguna tidak dibenarkan menukar maklumat yang terdapat pada *faceplate* (UTP port); (e) Semua kabel rangkaian hendaklah dipasang dengan kemas, melalui *conduit* dan bersesuaian; (f) Sebarang kerosakan pada kabel UTP atau masalah capaian rangkaian hendaklah dilaporkan kepada BTM; dan (g) Semua permohonan untuk mendapatkan sambungan rangkaian LADA mestilah mendapatkan kebenaran BTM.	
6.6.3 Pengurusan Alamat *Internet Protocol* (IP)	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna adalah dilarang sama sekali menukar konfigurasi IP di dalam komputer masing-masing tanpa kebenaran BTM; (b) Sebarang keperluan menggunakan IP statik hendaklah dipohon kepada BTM; dan (c) IP statik yang diberikan kepada pengguna tidak boleh digunakan untuk kepentingan sendiri. Sekiranya pengguna didapati menyalahgunakan IP statik, PC pengguna berkenaan akan dihalang daripada membuat capaian ke rangkaian LADA.	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
6.6.4 Talian Internet Persendirian	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kemudahan talian Internet persendirian dan seumpamanya hanya dibenarkan untuk tujuan rasmi dan mendapat kebenaran daripada BTM; (b) Pengguna hendaklah memutuskan (*disable/disconnect)* sambungan ke rangkaian LADA terlebih dahulu sebelum menggunakan talian Internet persendirian. Penggunaan talian persendirian dan rangkaian LADA secara serentak adalah dilarang; dan (c) Setelah menggunakan kemudahan tersebut pengguna dikehendaki mengimbas keseluruhan komputer yang digunakan sebelum menyambung semula ke rangkaian LADA bagi memastikan tiada virus masuk ke rangkaian LADA.	Semua
6.7 Pengurusan Media	
Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
6.7.1 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada ketua jabatan/pegawai yang diberi kuasa terlebih dahulu.	Semua
6.7.2 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Mengehadkan dan menentukan capaian media kepada pengguna yang sah sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; dan (f) Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	
6.7.3 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 sistem dokumentasi sedia ada.	Semua
6.8 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara LADA dan agensi luar terjamin.	
6.8.1 Pengurusan Mel Elektronik (E-mel)	
Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(a) Akaun e-mel bukanlah hak mutlak seseorang. Ia adalah kemudahan yang tertakluk kepada peraturan LADA dan boleh ditarik balik jika penggunaannya melanggar peraturan; (b) Warga LADA adalah bertanggungjawab kepada akaun e-mel masing-masing. LADA tidak akan bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan e-mel; (c) Pengguna wajib menggunakan e-mel rasmi kerajaan dalam urusan rasmi dan urusan pentadbiran harian. Penggunaan e-mel rasmi untuk tujuan komersial dan politik adalah tidak dibenarkan; (d) Warga LADA tidak dibenarkan menggunakan kemudahan e-mel percuma seperti Hotmail, Gmail dan Yahoo untuk tujuan rasmi; (e) Pengguna adalah dinasihatkan menggunakan kemudahan e-mel secara rutin sekurang-kurangnya sekali sehari; (f) Pengguna **TIDAK** dibenarkan menghantar maklumat Rahsia atau Rahsia Besar melalui e-mel; (g) Setiap akaun e-mel yang disediakan adalah untuk kegunaan individu berkenaan sahaja. Penggunaan akaun milik orang lain, memberi akaun kepada orang lain dan berkongsi akaun e-mel adalah dilarang; (h) Setiap bahagian dan unit hanya diperuntukkan satu e-mel bahagian sahaja berdasarkan keperluan dan kelulusan BTM LADA. Penghantaran e-mel menggunakan e-mel bahagian perlu menjelaskan nama, jawatan dan nombor untuk dihubungi bagi mengelakkan kesamaran dalam penggunaan e-mel bahagian. (i) Pengguna dilarang melakukan pencerobohan atau percubaan untuk menceroboh masuk ke mana-mana akaun pengguna lain;	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(j) Pengguna dilarang menghantar e-mel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian; (k) Pengguna dilarang menyebar perisian cetak rompak atau maklumat berbau politik, hasutan atau perkauman, bahan-bahan lucah, perjudian, jenayah atau apa-apa maklumat yang menyalahi undang-undang, menjejaskan reputasi LADA dan Perkhidmatan Awam melalui kemudahan e-mel LADA adalah dilarang; (l) Elakkan dari menerima dan membuka e-mel di mana penghantarnya tidak diketahui dan diragui dan pengguna perlulah memadam terus e-mel tersebut; (m) Saiz e-mel (*mailbox*) setiap pengguna adalah bergantung kepada kapasiti yang dibekalkan oleh BTM seperti berikut: i. Pengurusan Tertinggi – 50GB ii. Pengurus Bahagian dan Ketua Unit – 30GB iii. Gred 45 – 54 – 20GB iv. Gred 41 – 44 – 10GB v. Lain-lain gred – 3GB vi. E-mel berkapasiti rendah – 300MB (n) Saiz lampiran (*attachment*) yang dibenarkan adalah tidak melebihi 25 MB. Kaedah pemampatan dan kaedah muat turun fail dengan menggunalan *Universal Resource Location* (URL) untuk mengurangkan size adalah disarankan; (o) Pengguna adalah bertanggungjawab untuk mengurus dan memastikan saiz e-mel yang disimpan di dalam peti mel (*mailbox*) masing-masing tidak melebihi kuota yang telah ditetapkan; (p) Pengguna digalakkan menukar kata laluan masing-masing setiap tiga (3) bulan bagi mengelakkan kata laluan bocor kepada pihak yang tidak bertanggungjawab; (q) Pengguna dikehendaki merahsiakan kata laluan daripada pengetahuan orang lain;	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(r) Pengguna hendaklah menggunakan perisian penyulitan untuk menghantar dokumen dan maklumat terperingkat melalui emel;	
(s) Pengguna juga hendaklah memastikan fail yang akan dihantar atau yang diterima melalui kepilan (*attachment*) bebas dari virus dengan melakukan scanning dengan perisian antivirus;	
(t) Aktiviti *spamming*, penyebaran virus, bahan-bahan negatif dan surat berantai adalah dilarang. Jika didapati dilakukan oleh warga LADA akaun mereka boleh dibatalkan tanpa sebarang notis;	
(u) Koordinator ICT bahagian di LADA perlu memaklumkan sebarang perubahan status pengguna kepada Pentadbir e-mel jika terdapat pertukaran masuk dan keluar agensi, bersara, diberhentikan dan lain-lain bagi tujuan kawalan keselamatan dan pengemaskinian akaun pengguna LADA;	Koordinator ICT Bahagian
(v) Akaun e-mel yang tidak digunakan untuk tempoh melebihi 30 hari akan dibekukan penggunaannya dan seterusnya dihapuskan selepas tiga (3) bulan kecuali telah dimaklumkan kepada BTM;	Pentadbir Sistem ICT
(w) Capaian e-mel pengguna yang tidak lagi berkhidmat di LADA akan dihentikan serta-merta;	
(x) *Mail Relay* hanya boleh digunapakai untuk server/aplikasi dalaman agensi sahaja bagi tujuan keselamatan.	
(y) Pentadbir Sistem ICT berhak memasang sebarang jenis perisian atau perkakasan penapisan e-mel dan virus yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis, menyekat atau menghapuskan manamana e-mel yang disyaki mengandungi virus atau berunsur spamming daripada memasuki komputer; dan	
(z) Pihak Pengurusan atau Pentadbir Sistem ICT boleh memantau semua e-mel LADA jika perlu tanpa mendapat kebenaran warga LADA.	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
6.8.2 Pengurusan Media Sosial	
Perkara-perkara yang perlu dipatuhi di dalam memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi dan disebarkan melalui media sosial adalah seperti berikut: (a) Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara; (b) Tidak melibatkan penyebaran maklumat dan dokumen terperingkat; (c) Tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan; (d) Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; dan (e) Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan.	Semua
Pegawai yang bertanggungjawab mengendalikan kandungan media sosial rasmi perlulah memastikan keselamatan capaian media sosial dengan melaporkan penyalahgunaan kepada penyedia perkhidmatan media sosial (Contohnya: Facebook, Twitter, Instagram).	Pentadbir Media Sosial
6.9 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
6.9.1 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT LADA;	ICTSO

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian.	
6.9.2 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit *(audit trail)*. Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi tujuan pemeriksaan dan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh/masa aktiviti, rangkaian dan aplikasi yang digunakan;	Pentadbir Sistem Aplikasi dan Pentadbir Sistem ICT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(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 2007 dan Akta Arkib Negara 2003. Pentadbir Sistem ICT dan Pentadbir Sistem Aplikasi 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 daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
6.9.3 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 tidak sah seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem ICT
6.9.4 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	Pentadbir Sistem ICT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Pemantauan dan analisa log perlu dilaksanakan secara berkala; (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti *housekeeping* log perlu dilaksanakan secara berkala; (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan, dianalisis dan diambil tindakan sewajarnya; dan (f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam LADA atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	
6.10 Data Terbuka	
Objektif: Data Terbuka Sektor Awam adalah untuk meningkatkan kualiti dan ketelusan penyampaian perkhidmatan serta meningkatkan produktiviti negara melalui pemanfaatan data terbuka.	
6.10.1 Pengurusan Data Terbuka	
Pelaksanaan data terbuka LADA perlulah berasaskan tadbir urus dan aktiviti yang telah dipersetujui oleh Ketua Pegawai Eksekutif. Perkara-perkara yang perlu dilaksanakan adalah seperti berikut: (a) Menubuhkan struktur tadbir urus atau tadbir urus sedia ada untuk melaksanakan tugas dan aktiviti berkaitan data terbuka LADA; (b) Membangunkan Pelan Pelaksanaan Data Terbuka LADA;	CDO dan Pengurus IT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(c) Mengenal pasti set data Jabatan/Bahagian yang boleh dimuat naik atau dipaut ke Portal Data Terbuka Sektor Awam; dan (d) Membuat semakan semula pelaksanaan data terbuka dan menilai tahap penggunaannya.	
6.11 Peminjaman Peralatan ICT	
Objektif: Memastikan pengurusan peminjaman ICT dilaksanakan secara sistematik dan keselamatan peralatan sepanjang proses pinjaman.	
6.11.1 Pengurusan Peminjaman Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) BTM LADA menyediakan kemudahan pinjaman peralatan ICT bagi tujuan urusan rasmi sahaja; (b) Permohonan mestilah dibuat lima (5) hari bekerja sebelum tarikh penggunaan. Sebarang kelewatan permohonan boleh menyebabkan permohonan pinjaman ditolak; (c) Permohonan pinjaman mesti dibuat melalui Borang Pinjaman Peralatan ICT (Borang KEW PA 9) berserta dengan surat/memo urusan rasmi tersebut; (d) BTM akan meluluskan permohonan pinjaman mengikut jumlah peralatan ICT yang tersedia pada masa tersebut; (e) Peralatan yang dipinjam mestilah dijaga dengan rapi daripada sebarang kecurian dan kerosakan. Pegawai yang membuat peminjaman peralatan guna sama haruslah bertanggungjawab sepenuhnya terhadap keselamatan peralatan yang dipinjam; (e) Peminjam mestilah bertanggungjawab sepenuhnya terhadap sebarang kerosakan akibat kecuaian yang berlaku sepanjang tempoh peralatan dipinjam;	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(f) Sekiranya berlaku kehilangan, peminjam perlu melaporkan dengan kadar segera kepada pihak Bahagian Pengurusan Aset dan BTM LADA serta mengambil tindakan segera berdasarkan Tatacara Pengurusan Aset Alih Kerajaan; (g) Peminjaman peralatan ICT dari agensi luar perlu mendapat kelulusan Pengurusan Tertinggi LADA; (h) Tempoh maksimum pinjaman peralatan adalah selama lima (5) hari bekerja sahaja. Peminjam dikehendaki mengisi borang pinjaman (KEW PA 9) semula untuk melanjutkan tempoh pinjaman; (i) Bagi peminjaman untuk kegunaan rasmi semasa waktu pejabat, peminjam atau wakil hendaklah datang sendiri untuk mengambil, mengisi borang dan memulangkan peralatan tersebut daripada/kepada pihak BTM; (j) Peminjam perlu memaklumkan kepada pihak BTM sekiranya memerlukan bantuan BTM untuk memasang dan mengambil peralatan tersebut selepas tempoh pinjaman. Sekiranya tidak dimaklumkan, peminjam adalah bertanggungjawab untuk menguruskan urusan pemasangan dan pemulangan; (k) Peminjam dikehendaki memulangkan semula peralatan yang dipinjam mengikut tarikh pinjaman. Semua peralatan yang dipinjam mestilah dipulangkan dalam tempoh waktu pejabat; (l) Bagi kegunaan di LADA, sekiranya pemulangan tidak dapat dilakukan dalam tempoh waktu pejabat, peminjam dikehendaki memaklumkan kepada Polis Bantuan untuk menjaga peralatan ICT di lokasi tersebut; (m) Pihak BTM yang menguruskan proses pemulangan perlu memastikan peralatan dan perisian dalam keadaan baik dan begitu juga peminjam dikehendaki untuk memeriksa peralatan dan perisian yang diterima juga dalam keadaan baik;	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(n) Bagi pinjaman laptop, pengguna dari bahagian/unit yang telah dibekalkan kemudahan laptop perlu menggunakan laptop bahagian/unit tersebut. Permohonan pinjaman laptop ICT hanya boleh dilakukan sekiranya laptop bahagian/unit tidak tersedia pada tarikh yang ingin digunakan; (o) Jika penggunaan peralatan ICT memerlukan kepada pengangkutan dan kawalan keselamatan, peminjam adalah bertanggungjawab untuk menguruskan sendiri urusan tersebut; (p) BTM LADA berhak untuk membuat pemeriksaan mengejut dari masa ke semasa untuk memastikan peralatan yang dipinjamkan berada dalam keadaan baik; dan (q) Data/fail peminjam adalah tanggungjawab peminjam dan hendaklah dipadam sebelum pemulangan. Data/fail sulit (*confidential*) mestilah dipadam untuk mengelakkan daripada disalahgunakan oleh pihak yang tidak bertanggungjawab. BTM LADA tidak bertanggungjawab ke atas kehilangan atau penyalahgunaan data/fail peminjam yang di simpan dalam peralatan ICT yang dipinjamkan. BTM LADA akan memadam data/fail tersebut selepas peralatan ICT dipulangkan semula.	

PERKARA 7

KAWALAN CAPAIAN

PERKARA 7: KAWALAN CAPAIAN

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
7.1 Kawalan Capaian	
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT LADA.	
7.1.1 Keperluan Kawalan Capaian	
Capaian kepada sistem dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong polisi kawalan capaian pengguna sedia ada.	BTM
7.2 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT LADA	
7.2.1 ID Pengguna	
Pengguna adalah bertanggungjawab ke atas ID pengguna yang diberi untuk capaian sistem aplikasi. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: (a) ID pengguna yang diperuntukkan oleh LADA sahaja boleh digunakan. Penggunaan ID milik orang lain atau ID yang dikongsi bersama adalah dilarang; (b) ID pengguna mestilah unik; (c) ID pengguna yang diwujud 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 ID pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan LADA. ID boleh ditarik	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
balik jika penggunaannya melanggar peraturan; (e) Pentadbir Sistem Aplikasi harus menyemak ID pengguna dan hak aksesnya bagi menentukan ketepatan dan kesempurnaan sesuatu tahap capaian secara berkala; dan (f) Pentadbir Sistem Aplikasi berhak menggantung (*suspend*) dan menamatkan ID pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar atau dipinjamkan ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan.	
7.2.2 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian
7.2.3 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 LADA seperti berikut: (a) Pengguna baharu hendaklah memohon ID pengguna dengan mengisi borang yang disediakan; (b) Pengguna perlu menukar kata laluan setiap tiga (3) bulan; (c) Kata laluan hendaklah tidak dipaparkan semasa input; (d) Panjang kata laluan sekurang-kurangnya 8 aksara; (e) Kata laluan mesti menggunakan kombinasi daripada aksara huruf besar, aksara huruf kecil, angka dan simbol-simbol lain;	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(f) Kata laluan tidak boleh dikongsi dengan orang lain; (g) Menggunakan kata laluan yang selamat dan tidak mudah dicerobohi. Penggunaan kata laluan yang sukar diramal oleh penggodam adalah digalakkan; (h) Pengguna dilarang menggunakan kata laluan yang sama dengan ID pengguna; dan (i) Kata laluan hendaklah diingat dan tidak digalakkan dicatat, disimpan atau didedahkan dengan apa cara sekalipun.	
7.2.4 *Clear Desk 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 dokumen terperingkat terdedah sama ada atas meja kerja warga atau di paparan skrin komputer apabila tidak berada di hadapan komputer/tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Gunakan kemudahan *password screen saver* atau log keluar (*sign out*) apabila meninggalkan komputer; (b) Dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan (c) Set tetapan fungsi '*Lock Screen"* selepas lima (5) minit komputer tidak digunakan.	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
7.3 Keselamatan Internet	
Objektif: Melindungi aset ICT melalui sistem komunikasi Internet yang selamat.	
7.3.1 Internet	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh ketua jabatan/pegawai yang diberi kuasa; (b) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; (c) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengurusan Tertinggi sebelum dimuat naik ke Internet; (d) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; (e) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh LADA; (f) Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensiagensi Kerajaan”.	Semua
7.3.2 Melayari Internet	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna yang melayari aplikasi dan laman web adalah bertanggungjawab sepenuhnya ke atas maklumat yang dikunci masuk serta capaian yang dilakukan;	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Pengguna tidak dibenarkan menggunakan rangkaian *broadband* dan seumpamanya untuk melayari aplikasi dan laman web tanpa kebenaran daripada BTM; (c) Penghantaran dokumen yang mengandungi maklumat terperingkat (sulit atau terhad) melalui Internet hendaklah melalui proses penyulitan terlebih dahulu menggunakan perisian penyulitan yang disyorkan oleh BTM; (d) Pengguna adalah dilarang menyumbangkan perkara-perkara bertentangan dengan Perintah Am Kerajaan kepada mana-mana laman web tanpa kebenaran ketua jabatan; (e) Pengguna tidak dibenarkan membuat capaian kepada bahan-bahan terlarang seperti laman pornografi, perisian judi, permainan dan lain-lain yang melalaikan atau seumpamanya dengan menggunakan kemudahan pejabat; (f) Pada waktu pejabat, pengguna hanya dibenarkan membuat capaian kepada laman web jaringan sosial yang berkaitan dengan urusan rasmi agensi sahaja; (g) Capaian laman yang berbentuk hiburan, permainan komputer *online, radio online* dan *video streaming* yang membebankan rangkaian LADA adalah tidak dibenarkan; (h) Pengguna tidak dibenarkan melayari laman-laman yang tidak berkaitan dengan tugas di waktu pejabat; (i) Pengguna tidak dibenarkan melanggan kepada mana-mana *mailing list* yang tidak berkaitan dengan tugas; (j) Aktiviti perbincangan digital hanya dibenarkan untuk urusan rasmi dan perisian yang dibenarkan sahaja; (k) Aktiviti muat turun (*download*) atau muat naik (*upload*) sebarang perisian cetak rompak adalah dilarang; (l) Penggunaan sebarang perisian *Internet Proxy* untuk capaian ke Internet adalah tidak dibenarkan. Pentadbir Rangkaian berhak menyekat capaian ke Internet bagi PC	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
yang dikesan menggunakan perisian tersebut; (m) Pentadbir Sistem ICT adalah diberi kuasa untuk menjana laporan capaian rangkaian dan Internet setiap pengguna kepada pihak pengurusan; (n) Pentadbir Sistem ICT berhak menyediakan dan memasang perisian penapisan isi kandungan Internet; (o) Pentadbir Sistem ICT berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang tidak sesuai; dan (p) Kemudahan *wireless* LAN perlu dipastikan mempunyai kawalan keselamatan.	
7.4 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
7.4.1 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian kepada 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*;	ICTSO dan Pentadbir Sistem ICT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
dan (c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Mengehadkan dan mengawal penggunaan program; dan (d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
7.4.2 Kad Pintar/*Soft Cert*/Token	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG)/*Soft Cert*/Token hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; (b) Kad pintar/*Soft Cert*/Token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian kad pintar/*Soft Cert*/Token untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar/*Soft Cert*/Token yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan (d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pengeluar kad pintar/*Soft Cert*/Token.	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
7.5 Kawalan Capaian Sistem dan Aplikasi	
Objektif: Melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.	
7.5.1 Sistem Maklumat dan Aplikasi	
Capaian sistem dan aplikasi di LADA adalah terhad kepada pengguna dengan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; (c) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; (d) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (e) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (f) Untuk mengelakkan capaian terus secara fizikal kepada server yang berada di Pusat Data, capaian sistem maklumat dan aplikasi melalui jarak jauh (*remote*) adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada pegawai berkenaan dan perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem Aplikasi dan Pengguna Pentadbir Rangkaian

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
7.6 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan bagi komputer mudah alih dan kerja jarak jauh.	
7.6.1 Penggunaan Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Merekodkan aktiviti keluar masuk peralatan komputer mudah alih guna sama bagi memantau pergerakan peralatan tersebut; dan (b) Kabel keselamatan (*cable lock*) hendaklah dipasang pada peralatan mudah alih yang dibekalkan dengan kemudahan tersebut dan disimpan atau dikunci di tempat yang selamat apabila tidak digunakan.	Semua
7.6.2 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

PERKARA 8

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN

PERKARA 8: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
8.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
8.1.1 Keselamatan Aplikasi	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pembangunan sistem aplikasi harus mengambil kira keperluan aspek keselamatan yang ditetapkan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan bagi memastikan tidak wujud sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan seperti berikut: (c) Sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan; (d) Sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna; (e) Sistem output untuk memastikan data yang telah diproses adalah tepat; (f) Semua sistem aplikasi yang dibangunkan sama ada secara dalaman atau *outsource* hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan mematuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. Ujian tahap keselamatan harus merangkumi Penilaian Keterdedahan (*Vulnerability Assessment*) oleh pihak berkenaan sebelum pengaktifan sistem; (g) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan	Pemilik Sistem, Pentadbir Sistem Aplikasi dan Pentadbir Sistem ICT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(h) Pemilik Sistem perlu mengenalpasti sama ada maklumat dalam sistem aplikasi tersebut memerlukan penentusahan melalui Pengurusan Infrastruktur Kunci Awam (PKI) dan tandatangan digital.	
8.1.2 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
8.1.3 Kawalan 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) Memastikan keterdedahan ancaman maklumat teknikal diperolehi daripada pihak berkaitan; (b) Menilai tahap keterdedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Pentadbir Rangkaian
8.1.4 Kawalan Kod Sumber dan Dokumentasi Sistem Aplikasi	
Kawalan kod sumber dan dokumentasi sistem aplikasi hendaklah dilaksanakan ke atas sistem yang dibangunkan secara *outsource* dan *in-house*. Ini bagi memastikan kesinambungan sistem aplikasi itu dapat berjalan dengan lancar sama ada selepas pertukaran pegawai atau penyerahan sistem kepada Pemilik Sistem aplikasi.	Pentadbir Sistem Aplikasi

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan kod sumber dan dokumentasi bagi setiap sistem yang dibangunkan disediakan sama ada secara *hardcopy* dan/atau *softcopy*; (b) Dokumentasi bagi konfigurasi integrasi antara sistem induk dan aplikasi *mobile* disediakan; (c) Semua dokumentasi diletakkan secara berpusat, dikawal dan direkodkan; dan (d) Memastikan kod sumber sistem dan dokumentasi ialah hak milik Kerajaan.	
8.2 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
8.2.1 Penyulitan	
Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitif atau maklumat terperingkat (sulit atau terhad) sebelum dipindahkan keluar sama ada melalui e-mel, media storan atau lain-lain kaedah penghantaran.	Semua
8.2.2 Tandatangan Digital	
Penggunaan tandatangan digital adalah mengikut keperluan khususnya kepada mereka yang menguruskan transaksi maklumat terperingkat (sulit atau terhad) secara elektronik.	Semua
8.2.3 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
8.3 Pembangunan Sistem Aplikasi	
Objektif: Memastikan supaya pembangunan sistem diselia dan dipantau untuk memastikan ia mengikut jadual yang telah ditetapkan.	
8.3.1 Prosedur Pembangunan Sistem Aplikasi	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Bahagian dan Unit hendaklah memohon secara rasmi kepada BTM untuk membangunkan sesuatu sistem aplikasi melalui Pengurus Bahagian dan Unit masing-masing; (b) Kertas keperluan bisnes untuk membangunkan sistem aplikasi perlu disediakan dan mendapat kelulusan JPICT; (c) Bahagian perlu memohon kelulusan JPICT untuk membangunkan sistem aplikasi. Permohonan ini hendaklah lengkap meliputi spesifikasi teknikal, anggaran kos yang terlibat, guna tenaga dan juga skop perluasan sistem aplikasi tersebut; (d) Tempoh pembangunan sistem aplikasi adalah bergantung kepada kompleksiti sistem aplikasi. (e) Sistem aplikasi perlu mempunyai Pemilik (owner) iaitu sesuatu bahagian atau pengguna utama (yang paling banyak menggunakan sistem atau yang paling banyak memiliki data); (f) Pengguna yang bertukar bidang tugas atau tidak lagi berkhidmat di LADA akan dihapus ID dan capaiannya ke aplikasi dalam masa serta-merta; (g) Bahagian yang memohon akan menjadi Pemilik (*owner*) kepada sistem aplikasi tersebut dan hendaklah melantik *Champion* bagi melancarkan pelaksanaan sistem aplikasi. *Champion* yang dilantik dicadangkan daripada kalangan pegawai atasan bahagian/agensi. Pemilik juga bertanggungjawab mempromosi dan memastikan kejayaan pelaksanaan sistem;	Pentadbir Sistem Aplikasi dan Pengguna

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(h) Pengguna perlu membaca, memahami dan mematuhi prosedur menggunakan sistem melalui dokumen-dokumen yang disediakan; (i) Sistem aplikasi yang perlu diintegrasikan dengan sistem aplikasi yang lain hendaklah diterajui oleh Pemilik (*owner*) sistem aplikasi tersebut; (j) Pemilik (*owner*) sistem aplikasi perlu membuat pelaporan kepada JPICT secara berkala bagi kemajuan (*progress*) sistem aplikasi tersebut; (k) Pembangunan sistem aplikasi hendaklah mengambil kira sistem aplikasi sedia ada di agensi berkenaan dan agensi lain bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama. Sebagai contoh pembangunan sistem yang berkaitan sumber manusia hendaklah dielakkan kerana Sistem Pengurusan Sumber Manusia (HRMIS) telah sedia ada untuk diguna pakai; (l) Pembangunan sistem aplikasi mestilah mengguna pakai kod-kod yang standard di bawah Data Dictionary Sektor Awam (DDSA); (m) Pembangunan aplikasi yang melibatkan borang yang diwartakan perlulah mendapatkan kelulusan menteri yang berkenaan oleh Pemilik (*owner*) sesuatu sistem aplikasi; (n) Bahagian (pengguna utama) hendaklah memperuntukkan seorang atau lebih kakitangan sebagai wakil tetap yang dapat meluangkan masa yang cukup sepanjang proses pembangunan dan kerja-kerja berkaitan dengan projek; (o) Semua projek sistem aplikasi perlu mewujudkan Tadbir Urus Projek (Pasukan Projek, Jawatankuasa Teknikal dan Jawatankuasa Pemandu); (p) Bagi projek sistem aplikasi yang melibatkan lebih daripada satu (1) bahagian, maka setiap bahagian perlu mempunyai wakil tetap bagi menganggotai Pasukan Projek, Jawatankuasa Teknikal dan Jawatankuasa Pemandu;	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(q) Cadangan Sistem (*System Proposal*) perlu dibentangkan kepada pengguna/pemilik projek untuk ulasan dan persetujuan serta ditandatangani oleh pengguna/pemilik sistem; (r) Bagi sistem yang melibatkan fungsi dan prosedur tertentu, *Subject Matter Expert* (SME) perlu dilibatkan dalam mereka bentuk kawalan yang berkaitan dengan subject matter (contoh: Bagi sistem yang melibatkan fungsi dan prosedur kewangan, Akauntan perlu dilibatkan dalam mereka bentuk kawalan yang berkaitan dengan perakaunan); (s) Pengujian sistem di setiap peringkat (*unit testing, component testing, integration testing dan system testing*) perlu dibuat; (t) Pengujian Penerimaan Pengguna perlu dilaksanakan dan pengguna perlu menandatangani semua ujian penerimaan tersebut; (u) Pelaksanaan kawalan keselamatan ICT dalam aplikasi adalah perlu bagi menghalang capaian yang tidak sah, ubahsuaian, penyebaran maklumat dan kerosakan maklumat; (v) *Source code* dan hak cipta bagi sesuatu aplikasi yang dibangunkan secara dalaman ataupun secara bersama dengan pembekal perlu dinyatakan dalam kontrak sebagai Hak Kerajaan Malaysia; (w) Bagi aplikasi yang dibangunkan oleh pembekal, klausa mengenai pemindahan teknologi (*Transfer of Technology*) hendaklah dinyatakan dalam dokumen kontrak; dan (x) Dokumentasi sistem hendaklah disediakan bagi semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya.	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
8.3.2 Perubahan / Keperluan Tambahan Sistem Aplikasi Sedia Ada	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Spesifikasi keperluan sistem aplikasi yang telah dipersetujui, tetapi memerlukan perubahan atau tambahan keperluan hendaklah dimohon secara bertulis atau menggunakan borang permohonan yang disediakan; dan	Pemilik Sistem
(b) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Pentadbir Sistem Aplikasi
8.4 Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
8.4.1 Kawalan Fail Sistem	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem Aplikasi 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) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; (d) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan (e) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang dibenarkan.	Pentadbir Sistem Aplikasi, Pentadbir Sistem ICT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
8.5 Pembayaran *Online*	
Objektif: Menerangkan dengan lebih terperinci prosedur yang perlu dipatuhi dalam proses pembayaran online di dalam sistem.	
8.5.1 Pembayaran *Online* bagi Sistem Aplikasi	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pemilik Sistem perlu menentukan kaedah pembayaran pada sistem aplikasi iaitu secara *direct debit* menggunakan *payment gateway Financial Process Exchange* (FPX) atau/dan menggunakan kad kredit; (b) Pemilik Sistem perlu mendapatkan kelulusan Jabatan Akauntan Negara Malaysia (JANM) untuk pelaksanaan pembayaran secara *online* melalui sistem aplikasi; (c) Pemilik Sistem perlu mendapatkan kelulusan daripada JANM bagi pembukaan akaun bank di *acquiring bank*; (d) Dokumen perjanjian antara LADA dan *acquiring bank* mesti disediakan dan ditandatangani selaras dengan Pekeliling Perbendaharaan semasa yang sedang berkuatkuasa; (e) Pemilik Sistem perlu mempunyai peruntukan kewangan yang mencukupi bagi membiayai caj perkhidmatan yang dikenakan oleh bank dalam memproses bayaran secara online selaras Pekeliling Perbendaharaan semasa yang sedang berkuatkuasa; (f) Pemilik Sistem hendaklah memastikan segala terimaan harian dipindahkan ke Akaun Terimaan Kerajaan (Akaun Bank Pejabat Perakaunan) pada keesokan harinya sebelum jam 4 petang; (g) Pemilik Sistem hendaklah memastikan laporan Urusniaga dari bank adalah sama dengan sistem; dan	Pemilik Sistem

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(h) Sistem yang dibangunkan perlu direkabentuk menggunakan fungsi *Public Key Infrastructure* (PKI).	Pembangun Sistem
8.6 Penamatan Sistem	
Objektif: Menerangkan prosedur yang perlu dilakukan apabila ingin menamatkan penggunaan sesuatu sistem	
8.6.1 Penamatan Penggunaan Sistem Aplikasi	
Perkara yang perlu dipatuhi adalah seperti berikut:	
(a) Pemilik Sistem perlulah memaklumkan secara bertulis kepada Pengurus ICT sekiranya tidak lagi memerlukan/ menggunakan sistem aplikasi; dan	Pemilik Sistem
(b) Sekiranya sesebuah sistem aplikasi tidak digunakan langsung untuk tempoh dua (2) tahun, Pengurus IT boleh mencadangkan kepada bahagian agar sistem aplikasi tersebut ditamatkan penggunaannya.	Pengurus IT
8.7 Laman Web	
Objektif: Menerangkan perkara-perkara yang perlu dipatuhi dalam membangunkan laman web di LADA.	
8.7.1 Pengurusan Laman Web	
Perkara yang perlu dipatuhi adalah seperti berikut:	
(a) Kandungan laman web berikut adalah di bawah seliaan Unit Khidmat Korporat, Bahagian Pelancongan dan Bahagian Perancangan LADA: i. LADA - https://www.lada.gov.my ii. Langkawi Geopark - https://langkawigeopark.com.my iii. Naturally Langkawi – https://naturallylangkawi.my iv. Taman Lagenda - https://lagenda.lada.gov.my/	Koordinator Web

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(b) Semua maklumat yang hendak dimuatkan ke dalam laman web mestilah mendapat kelulusan KPE melalui Unit Khidmat Korporat LADA; (c) Maklumat yang terkandung dalam laman web adalah di bawah tanggungjawab bahagian masing-masing; (d) Laman web/portal syarikat atau individu yang memerlukan pautan ke laman web LADA atau sebaliknya mestilah mendapat kebenaran KPE. (e) Tadbir urus laman web LADA khususnya yang berkaitan dengan kandungan diselaraskan melalui Jawatankuasa Pengurusan Laman Web LADA berdasarkan Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 Pengurusan Laman Web Agensi Sektor Awam; (f) Pihak pentadbir bagi semua laman web perlu memastikan setiap isi kandungan laman web dikemaskini mengikut keperluan semasa; (g) Kandungan laman web tidak boleh mengandungi sebarang unsur menyalahi yang menyalahi undang-undang; (h) Semua kualiti imej dan gambar akan disaring oleh BTM LADA sebelum dimuatnaik ke laman web bagi memastikan menepati standard yang ditetapkan; (i) Berikut merupakan tempoh pengemaskinian maklumat yang perlu dipantau oleh pentadbir laman web LADA: i. Tarikh kemaskini laman web perlu sentiasa dipaparkan berdasarkan tarikh pengemaskinian; ii. Berita/aktiviti/peristiwa - tarikh pengemaskinian mestilah tidak melebihi satu (1) bulan. Sebarang pengemaskinian maklumat perlu diserahkan kepada BTM dalam tempoh tiga (3) hari sebelum tarikh aktiviti/peristiwa berlangsung;	

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
iii. Hebahan/makluman/pengumuman - tarikh yang dikemaskini tidak melebihi tiga (3) hari bekerja bagi jenis kandungan biasa. Abaikan jenis kandungan jika berterusan; iv. Poster/banner - tarikh yang dikemaskini tidak melebihi 1 minggu bagi jenis kandungan biasa. Abaikan jenis kandungan jika berterusan; v. Bilangan transaksi dalam talian - maklumat sekurang-kurangnya dua (2) bulan dari bulan semasa. Abaikan jenis kandungan jika berterusan; vi. Sebutharga/Tender/Jawatan Kosong - Tarikh tutup tidak melebihi satu (1) hari bekerja; dan vii. Maklumat Anggota Pentadbir dan Pengurusan Atasan - Memastikan maklumat terkini anggota pentadbir dan pengurusan tertinggi adalah terkini.	
8.8 Multimedia	
Objektif: Menerangkan perkara-perkara yang perlu dipatuhi dalam penyediaan rekaan grafik dan multimedia di LADA.	
8.8.1 Pengurusan Multimedia	
(a) Semua kategori rekabentuk grafik dan multimedia akan disediakan dalam tempoh maksimum tiga (3) minggu selepas maklumat lengkap diperolehi. (b) Permohonan rekabentuk multimedia perlu menggunakan Borang Permohonan Multimedia ICT seperti di Lampiran 2. (c) Pemohon perlu menyediakan maklumat dan bahan yang lengkap bagi melancarkan proses penyediaan rekabentuk ini. (d) Bagi penyediaan montaj/video, pemohon perlu mengemukakan cadangan idea asas bagi membolehkan	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
pihak IT mendapat konsep idea yang jelas sebelum pembangunan montaj/video dilaksanakan. (e) Proses penambahbaikan montaj/video tidak akan dilakukan dalam tempoh dua (2) hari sebelum acara berlangsung.	
8.9 Pembangunan Aplikasi *Mobile*	
Objektif: Menerangkan perkara-perkara yang perlu dipatuhi dalam membangunkan aplikasi *mobile*.	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pembangunan aplikasi *mobile* mestilah menggunakan API sebagai antara muka hubungan dengan sistem induk; dan (b) Sistem aplikasi *mobile* yang dibangunkan perlu melalui akaun langganan GAMMA untuk dimuat naik ke Apps Market Place. (Contohnya: Apple App Store, Google Play).	Pentadbir Sistem ICT

PERKARA 9

PENGURUSAN PENGENDALIAN INSIDEN

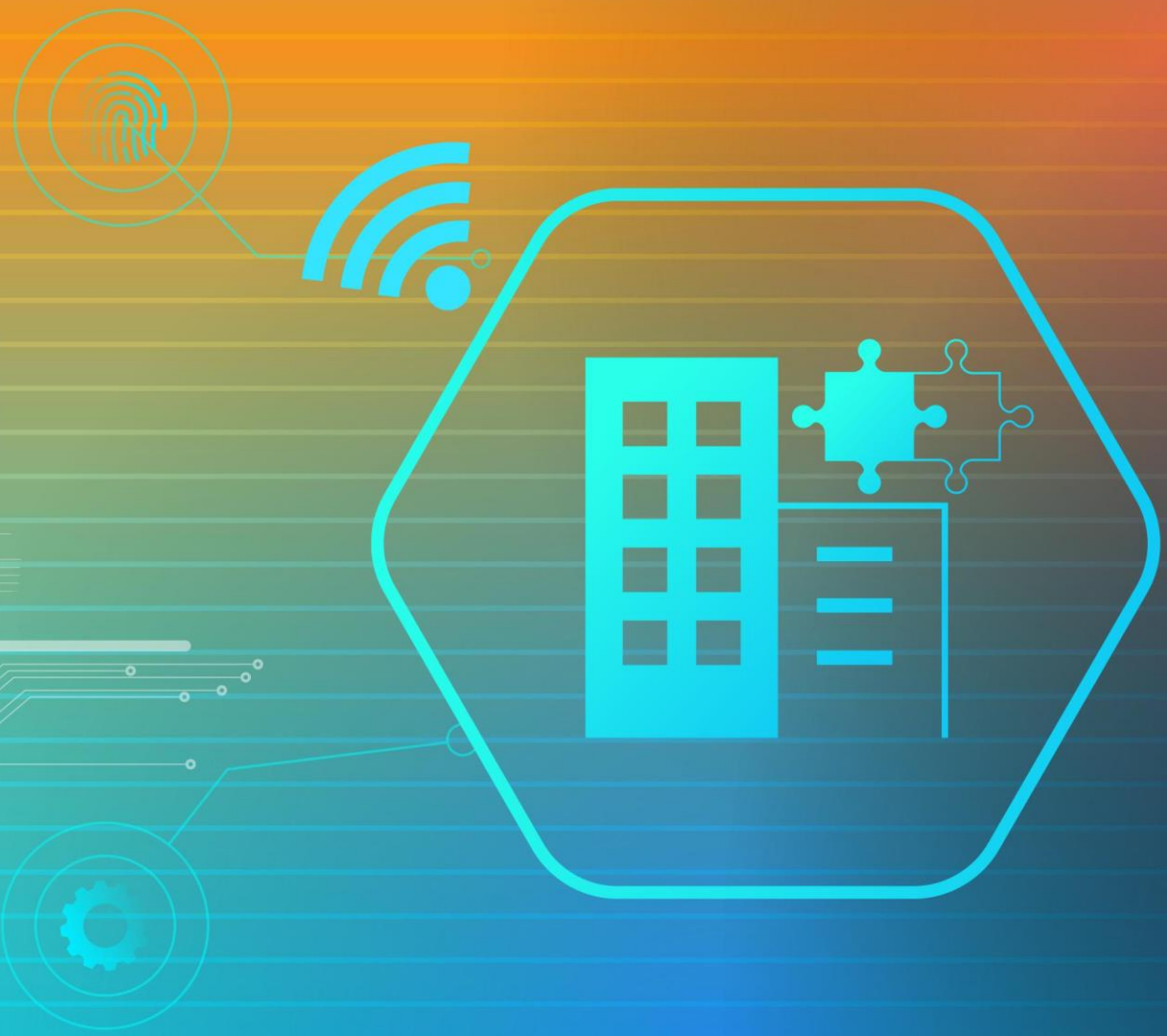
PERKARA 9: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
9.1 Menangani Insiden Keselamatan ICT	
Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
9.1.1 Mekanisma Pelaporan Insiden Keselamatan Siber	
Semua insiden keselamatan siber yang berlaku mesti dilaporkan segera kepada ICTSO untuk pengendalian dan pengumpulan statistik insiden keselamatan siber bagi mengelakkan kerosakan bahan bukti tanpa melaksanakan tindakan secara sendirian. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. Antara insiden keselamatan siber yang perlu dilaporkan adalah: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri, didedahkan atau disyaki hilang; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi”; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam”.	Semua

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
9.2 Prosedur Pengurusan dan Pengendalian Insiden Keselamatan Siber	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
9.2.1 Prosedur Pengurusan Insiden	
Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: (a) Menerima aduan insiden dari pengguna; (b) Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; (c) Menyedia pelan kontingensi dan mengaktifkan Pelan Pemulihan Bencana (DRP); (d) Menyimpan jejak audit dan memelihara bahan bukti; (e) Menyediakan tindakan pemulihan segera; (f) menyediakan tindakan pencegahan supaya insiden serupa tidak berulang; dan (g) memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	BTM

PERKARA 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN KESELAMATAN ICT



PERKARA 10: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
10.1 Kesinambungan Perkhidmatan	
Objektif: Menjamin operasi perkhidmatan ICT agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
10.1.1 Pelan Kesinambungan Perkhidmatan ICT	
Pelan Kesinambungan Perkhidmatan (PKP) 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 KPE LADA. Perkara-perkara berikut perlu diberi perhatian: (a) Pelan Kesinambungan Perkhidmatan LADA harus dibentuk dengan menggunakan pendekatan "berpasukan" di mana pasukan tersebut harus diwakili oleh semua bahagian di LADA; (b) Penilaian kegagalan keselamatan dan kerugian dalam perkhidmatan akibat bencana harus dianalisa; (c) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (d) Perancangan kecemasan harus dibina dan dilaksanakan untuk memastikan proses operasi boleh dijalankan semula di dalam tempoh masa yang diperlukan. Perancangan tersebut harus diselenggara dan diamalkan untuk menjadi asas proses pengurusan yang lain; (e) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam tempoh yang telah ditetapkan; (f) Mendokumentasikan proses dan prosedur yang telah dipersetujui;	CDO, BTM

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
(g) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (h) Membuat penduaan; dan (i) Menguji, membuat simulasi dan mengemaskini pelan sekurang-kurangnya setahun sekali.	
10.1.2 Kompetensi Digital	
Perancangan atau pelan latihan ICT adalah penting dalam memastikan kesinambungan perkhidmatan dan mestilah dirangka bagi memenuhi aspek seperti berikut: (a) Peningkatan Kompetensi Aplikasi Digital Latihan ini bertujuan untuk memantap dan meningkatkan kompetensi digital kakitangan dalam menggunakan aplikasi dalaman LADA. (b) Peningkatan Kepakaran Teknikal Latihan ini memfokuskan kepada peningkatan kompetensi teknikal di kalangan kakitangan dan personel ICT bagi memastikan semua latihan dan pensijilan yang diterima adalah bersesuaian (c) Peningkatan Kompetensi Digital Kakitangan Peningkatan Kompetensi Digital Kakitangan adalah untuk memastikan kakitangan mahir dalam pengunaan perisian seperti perisian automasi pejabat dan reka bentuk. (d) Pengiktirafan Personel ICT Program pengiktirafan Teknologis Profesional dan *Qualified Technician* adalah untuk mengiktiraf personel IT dalam bidang kemahiran teknikal.	BTM dan Semua

PERKARA 11

PEMATUHAN

PERKARA 11: PEMATUHAN

PERNYATAAN POLISI	PERANAN/ TANGGUNGJAWAB
11.1 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran kepada PKS LADA**.**	
11.1.1 Pematuhan Polisi	
Setiap pengguna di LADA hendaklah membaca, memahami dan mematuhi PKS LADA serta undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Setiap Pengguna hendaklah menandatangani Surat Akuan Pematuhan PKS LADA seperti di Lampiran 1. Semua aset ICT di LADA termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan ketua agensi berhak untuk memantau aktiviti Pengguna untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan.	Semua
11.1.2 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di LADA adalah seperti di Lampiran 3.	Semua
11.1.3 Perlanggaran Polisi	
Pelanggaran PKS LADA akan dikenakan tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-Perintah Am Bab D – Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib). Kemudahan ICT juga akan dilucutkan jika penggunaannya melanggar peraturan/ PKS LADA.	Semua

LAMPIRAN

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
LEMBAGA PEMBANGUNAN LANGKAWI

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian / Unit : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya telah membaca, memahami dan akur akan peruntukan – peruntukan yang telah terkandung di dalam Polisi Keselamatan Siber Lembaga Pembangunan Langkawi (LADA) ; dan

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

Tandatangan : .....

Tarikh : .....

Pengesahan TKPE (P)

.....
( )
b/p : Ketua Pegawai Eksekutif LADA

Tarikh : .....

BAHAGIAN TEKNOLOGI MAKLUMAT
BORANG PERMOHONAN REKABENTUK MULTIMEDIA

MAKLUMAT PEMOHON

Nama Pemohon	:	No. Telefon	:
Bahagian / Unit	:	Emel	:

PERINCIAN REKABENTUK MULTIMEDIA

Tajuk / Nama Program	:
Tarikh Program	:
Masa Program	:
Lokasi Program	:

Kategori Multimedia

- ☐ Hebahan Media Sosial
- ☐ Web Banner
- ☐ LED Panel
- ☐ Booklet
- ☐ Bunting : Saiz 2 ft X 6 ft
- ☐ Banner : _____ inci/mm/px X _____ inci/mm/px
- ☐ Backdrop (Projektor / Cetakan) : _____ inci/mm/px X _____ inci/mm/px
- ☐ Montaj : Durasi minit :_____
- ☐ Video/Audio : Durasi minit :_____
- ☐ Slaid Power Point : Ratio 4:3 / 16:9 (Sila bulatkan)
- ☐ Lain-lain (sila nyatakan) :

Logo Yang Diperlukan	:
Lain-lain maklumat : *(tagline / wording / gambar / informasi / contact)*	
Tarikh Rekabentuk Multimedia Diperlukan :	

UNTUK KEGUNAAN BAHAGIAN TEKNOLOGI MAKLUMAT

Staf IT yang terlibat :	
Tarikh Rekabentuk Multimedia Siap :	
Pengesahan Pengurus (IT) :	

SENARAI PERUNDANGAN DAN PERATURAN

1. Akta Aktiviti Kerajaan Elektronik 2007;
2. Akta Arkib Negara 2003
3. Akta Hak Cipta (Pindaan) Tahun 1997;
4. Akta Jenayah Komputer 1997;
5. Akta Komunikasi dan Multimedia 1998;
6. Akta Rahsia Rasmi 1972;
7. Akta Tanda Tangan Digital 1997;
8. Arahan Keselamatan;
9. Arahan No.24 Majlis Keselamatan Negara (MKN) – Dasar dan Mekanisme Pengurusan Krisis Siber Negara;
10. Arahan Perbendaharaan;
11. Arahan Teknologi Maklumat 2007;
12. Dasar Keselamatan ICT Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU) Jabatan Perdana Menteri 24 Mei 2010 Versi 5.3
13. Malaysian Personal Data Protection Act (MPDPA) 2010;
14. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
15. Open-Source Software (OSS) Implementation Guidelines August 2008;
16. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
17. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
18. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”;
19. Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 – Pengurusan Laman Web Agensi Sektor Awam;
20. Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 – Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan;
21. Pekeliling Perbendaharaan Pungutan Hasil Dan Terimaan Bukan Hasil Secara Online PS 2.2/2013;
22. Perintah-Perintah Am;
23. Perolehan Kerajaan PK 1/2013, Punca Kuasa, Prinsip dan Dasar Perolehan Kerajaan, Para 4: Perancangan Perolehan Tahunan Bagi Perolehan Secara

Tender Yang Menggunakan Peruntukan Persekutuan di Bawah Belanja Mengurus dan Pembangunan;

24. Perolehan Kerajaan PK 2/2013: Garis Panduan Mengenai Pengurusan Perolehan Information Telecommunication Technology (ICT) Kerajaan;
25. Perolehan Kerajaan PK 3.1/2013, Perolehan Perkhidmatan Perunding;
26. Polisi ICT LADA;
27. Polisi ICT Perbendaharaan;
28. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) Versi 1.0 April 2016
29. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
30. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
31. Surat Arahan Ketua Pengarah MAMPU - Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC27001:2007 dalam Sektor Awam bertarikh 24 Nov 2010
32. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam bertarikh 24 Nov 2010
33. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Risiko Keselamatan Maklumat Menggunakan MyRAM App 2.0 di Agensi Sektor Awam
34. Surat Arahan Ketua Pengarah MAMPU - Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di AgensiAgensi Kerajaan bertarikh 23 Mac 2009
35. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
36. Surat Arahan Ketua Setiausaha Negara – Langkah-langkah untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-agensi Kerajaan yang bertarikh 20 Oktober 2006;
37. Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
38. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

39. Surat Pekeliling Am Bilangan 3 Tahun 2015 – Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam;
40. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
41. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam;
42. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
43. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019
44. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019
45. The Malaysian Government Interoperability Framework for Open-Source Software (MyGIFOSS);