POLISI KESELAMATAN SIBER

VERSI 1.0

LEMBAGA PELABUHAN JOHOR
JOHOR PORT AUTHORITY

07 - 253 4000
admin@lpj.gov.my
www.lpj.gov.my

POLISI KESELAMATAN SIBER

KAWALAN (BERDASARKAN STANDARD MS ISO/IEC 27001:2022)

LAMPIRAN

GLOSARI

Perkara	Keterangan
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM untuk sebarang kemungkinan adanya 'virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
***Backup* (Sandaran)**	Proses penduaan sesuatu dokumen atau maklumat
Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
Bandwidth	Jalur Lebar. Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
***BCP*/PKP**	*Business Continuity Planning* Pelan Kesinambungan Perkhidmatan
CCTV	*Closed-Circuit Te/evision System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CIA	*Confidentiality, Integrity, Availability*
CDO	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan maklumat digital bagi menyokong arah tuju sesebuah organisasi.

Perkara	Keterangan
Clear Desk dan Clear Screen	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
Denial of service	Halangan pemberian perkhidmatan
Defence-in-depth	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
Downloading	Aktiviti muat turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
***Escrow* (eskrow)**	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/ espionage*), penipuan (*hoaxes*).
***CSIRT* LPJ**	*Computer Security and Incident Response Teams* atau Pasukan Tindak Balas Keselamatan Siber LPJ.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk

Perkara	Keterangan
	bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
LPJ	Lembaga Pelabuhan Johor
PPB	Penolong Pengurus Besar
STM	Sumber Teknologi Maklumat
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan siber.

1.0 TUJUAN

Polisi Keselamatan Siber LPJ ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusandengan perkhidmatan ICT dalam melindungi maklumat di ruang siber.

2.0 LATAR BELAKANG

Polisi ini dibangunkan untuk menjamin kesinambungan urusan LPJ dengan meminimumkan kesan insiden keselamatan siber. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi LPJ bagi memastikan semua maklumat dilindungi.

3.0 PENGENALAN

Polisi Keselamatan Siber (PKS) menerangkan peraturan, tindakan kawalan keselamatan siber serta tanggungjawab dan peranan warga LPJ, pembekal, perunding dan pihak ketiga yang mesti dibaca, difahami dan dipatuhi dalam melindungi aset ICT di ruang siber LPJ.

Ruang siber ditakrifkan sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset berkaitan ICT.

4.0 OBJEKTIF

Objektif utama PKS ini dibangunkan adalah seperti yang berikut:

a) Menerangkan kepada semua pengguna merangkumi warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber;

b) Memastikan keselamatan penyampaian perkhidmatan LPJ di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

c) Memastikan kelancaran operasi LPJ dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

d) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

e) Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

5.0 PENYATAAN POLISI

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

Pernyataan ini merangkumi perlindungan kepada semua bentuk **maklumat elektronik ataupun cetakan** bagi tujuan menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan.

CIRI CIRI UTAMA KESELAMATAN MAKLUMAT :

KESAHIHAN

- Data dan maklumat hendaklah dipasti kesahihannya

KETERSEDIAAN

- Data dan maklumat boleh diakses bila-bila masa apabila diperlukan

TIDAK DAPAT DISANGKAL

- Data dan maklumat hendaklah daripada sumber yang sah dan tidak boleh disangkal

KERAHSIAAN

- Maklumat dan data tidak boleh didedahkan sewenang-wenangnya dan diakses tanpa kebenaran

INTEGRITI

- Data dan maklumat hendaklah tepat, lengkap dan kemaskini dan hanya boleh diubah dengan cara yang dibenarkan

6.0 TADBIR URUS

Pembangunan PKS ini dilaksanakan oleh Unit Sumber Teknologi Maklumat (USTM) dan disahkan di dalam Mesyuarat JPICT Jabatan.

7.0 ASET ICT

Polisi ini meliputi semua sumber atau aset ICT yang digunakan seperti :

7.1 Maklumat

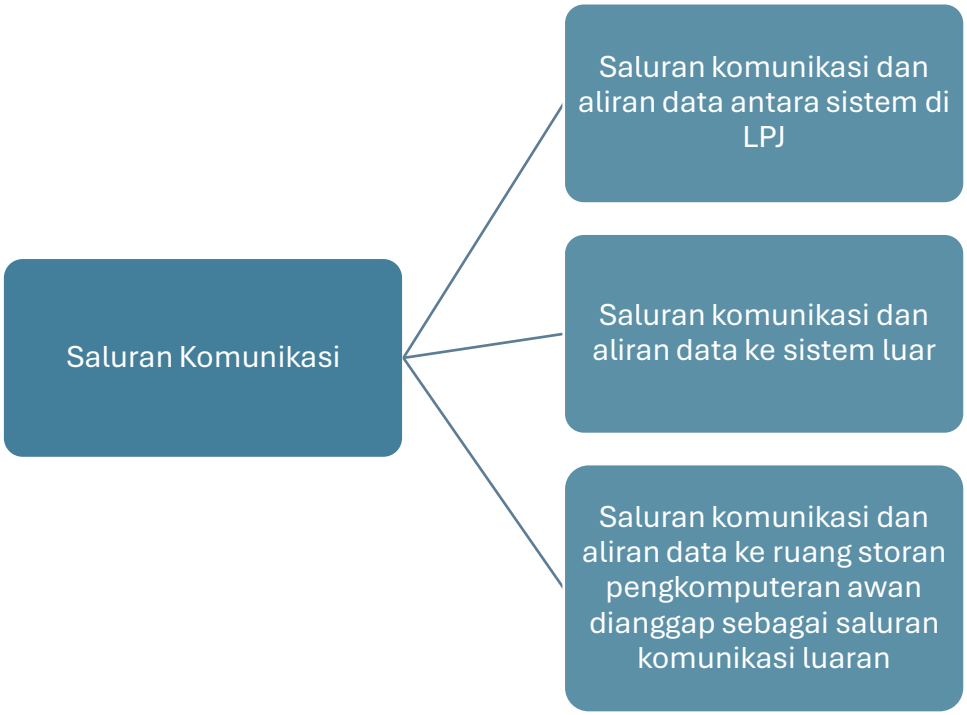
Semua penyedia perkhidmatan dalam LPJ hendaklah mengenai pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

Kategori	Keterangan
Maklumat Rahsia Rasmi	Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.
Maklumat Rasmi	Maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh LPJ semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang

Kategori	Keterangan
	tertakluk di bawah peraturan-peraturan Arkib Negara.
Maklumat Pengenalan Peribadi	Maklumat Pengenalan Peribadi (PII atau Personally Identifiable Information) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenai pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.
Data Terbuka	Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. PII dikecualikan daripada data terbuka.

7.2 Aliran Data

Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi dalam LPJ hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:



7.3 Platform Aplikasi dan Perisian

Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

7.4 Peranti Fizikal dan Sistem

Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

Pelayan/Server
- Fizikal/VM

Peranti/Peralatan Rangkaian
- Switch

Komputer Peribadi/Riba

Telefon/Peranti Pintar

Media Storan
- Hard Disk

Peranti dengan sambungan ke rangkaian
- Pengimbas
- Pencetak
- Sistem Kawalan Access
- CCTV

Peranti peribadi

Peranti pengesahan *(authentication device)*
- Token keselamatan
- Dongle
- Alat pengimbas biometrik

7.5 Sistem Luaran

Sistem luaran ialah sistem bukan milik LPJ yang dihubungkan dengan sistem LPJ. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

7.6 Sumber Luaran

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi LPJ. Contoh perkhidmatan sumber luaran ialah:

Perkhidmatan Sumber Luaran				
Perisian Sebagai Satu Perkhidmatan (SAAS)	Platform Sebagai Satu Perkhidmatan (PAAS)	Infrastruktur Sebagai Satu Perkhidmatan (IAAS)	Storan Pengkomputeran Awan (Cloud)	Pemantauan Keselamatan

Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala.

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

8.0 RISIKO

LPJ hendaklah mengenai pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian LPJ tidak dapat melaksanakan fungsi jabatan dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber LPJ.

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber LPJ.

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

a) Kerentatan	Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.
b) Ancaman	LPJ hendaklah mengenai pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.
c) Impak	LPJ hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi LPJ.
d) Tahap Risiko	Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

e) Penguraian Risiko

Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya. Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

Manusia	Mengenai pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.
Teknologi	Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, tembok api *(firewall)* digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.
Proses	Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

f) Pengurusan Risiko

Penyedia perkhidmatan digital di LPJ hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

- mengenai pasti kerentanan;
- mengenai pasti ancaman;
- menilai risiko;
- menentukan penguraian risiko;
- memantau keberkesanan penguraian risiko; dan
- memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

9.0 PRINSIP KESELAMATAN

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber LPJ dan perlu dipatuhi adalah seperti berikut:

a) **Prinsip "Perlu Tahu"**

LPJ hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip "Perlu Tahu" yang membenarkan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja.

Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkankepada masa, lokasi, peranan dan fungsi pengguna tersebut.

b) **Hak Keistimewaan Minimum**

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap 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. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari

semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

c) **Pengasingan Tugas**

Bagi mengekalkan prinsip sekat-dan-imbang (*check and balance*), LPJ hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

d) **Kawalan Capaian Berdasarkan Peranan**

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

e) **Peminimuman Data**

LPJ hendaklah mengamalkan prinsip peminimuman data yang mengehadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

10.0 TEKNOLOGI

Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data di setiap elemen pengkomputeran seperti berikut:

Peringkat Pemprosesan Data

- **Data Dalam Simpanan**

  LPJ hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.

  Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

- **Data Dalam Pergerakan**

  LPJ hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi 'data dalam pergerakan'.

- **Data Dalam Penggunaan**

  LPJ hendaklah menggunakan teknologi yang bersesuaian untuk melindungi 'data dalam penggunaan' bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

Teknologi yang bersesuaian boleh digunakan untuk memastikan asal data dan data/transaksi tanpa-sangkal.

Perlindungan Ketirisan Data

a) Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.
b) Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, LPJ hendaklah menggunakan kaedah teknologi dan kawalan keselamatan *(countermeasure* dan *control measure)* yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan yang dikeluarkan oleh Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan dari CGSO.

Setiap projek ICT yang dibangunkan di LPJ hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinciberhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

- **Peranti Pengkomputeran Peribadi**
  a) Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan

sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet dan peranti storan.

b) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada LPJ. Walau bagaimanapun, peranti pengkomputeran peribadi milik pensendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

- **Peranti rangkaian**

a) merujuk kepada peranti yang digunakan untuk membolehkan saling hubungantara peranti komputer dan sistem seperti suis, penghala, tembok api *(firewall)* , peranti VPN dan kabel.

b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

- **Aplikasi**

a) Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.

b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan,

data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

- **Pelayan**

a) Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

- **Persekitaran Fizikal**

a) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

b) LPJ hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

c) Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.

d) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat *defence-in-depth*.

11.0 PROSES

Warga LPJ hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

Proses	Keterangan
Konfigurasi Asas	a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem. b) Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.
Kawalan Perubahan Konfigurasi	a) Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi. b) Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini. c) Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan
Kawalan Perubahan Konfigurasi	a) Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

Proses	Keterangan
	b) Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini. c) Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.
Sandaran	a) Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan. b) Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.
Kitaran Pengurusan Aset	**<u>Pindah</u>** a) Pemindahan hak milik aset berlaku dalam keadaan berikut: i) Warga LPJ meninggalkan agensi disebabkan oleh persaraan, peletakan jawatan atau penugasan semula; ii) Aset yang dikongsi untuk kegunaan sementara; iii) Pemberian aset kepada agensi lain; dan iv) Aset dikembalikan setelah tamat tempoh sewaan. b) Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (2).

Proses	Keterangan
	Pelupusan a) Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya. b) Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377 [Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008] c) Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data. d) Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa. **Kitaran Hayat** a) Kitaran hayat data hendaklah diuruskan mengikut Akta 629. b) Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

12.0 MANUSIA

Warga LPJ, pembekal, pakar runding dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

Sistem penyampaian perkhidmatan LPJ hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan pengguna hendaklah dibangunkan bagi semua Warga LPJ.

Kompetensi Pengguna

Kompetensi pengguna termasuk:

a) Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT danprogram kesedaran keselamatan siber.

b) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada Warga LPJ berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

c) Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

d) Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

Kompetensi Pelaksana

a) Warga LPJ yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

b) Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

i) Mempunyai kelayakan akademik dalam bidang berkaitan atau sijilprofesional keselamatan siber.

ii) Memenuhi keperluan pembelajaran berterusan.

iii) Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.

iv) Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

c) Pegawai Keselamatan ICT yang dilantik hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di LPJ.

Peranan

a) Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

b) Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinanasal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

c) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.

d) Warga LPJ yang berperanan menguruskan aset ICT hendaklahmemastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.

e) Warga LPJ yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.

f) Warga LPJ yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan.

13.0 PELAN PENGURUSAN KESELAMATAN MAKLUMAT

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

Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

Kerahsiaan

- Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

Integriti

- Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan.

Tidak Boleh Disangkal

- Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

Kesahihan

- Data dan maklumat hendaklah dipastikan kesahihannya.

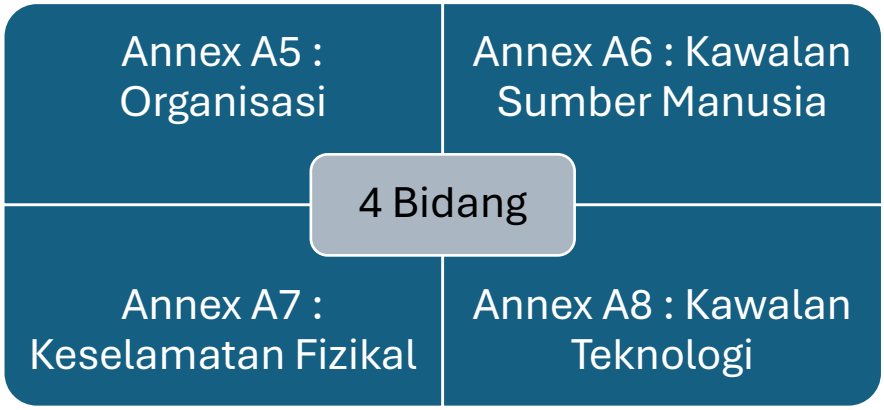
Ketersediaan

- Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT LPJ, ancaman yang wujud akibat daripada kelemahan

tersebut, risiko yang mungkin timbul danlangkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

EMPAT Bidang Keselamatan yang terlibat di dalam Polisi Keselamatan Siber LPJ diterangkan dengan lebih jelas dan teratur dalam dokumen ini.



ANNEX A **5**	**ANNEX A5 : KAWALAN ORGANISASI** ***(ORGANIZATIONAL CONTROL)***

5.1: POLISI KESELAMATAN MAKLUMAT *(POLICIES FOR INFORMATION SECURITY)*	
PERKARA	**PERANAN**
Pelaksanaan polisi ini akan dijalankan oleh Ketua Jabatan (KJ) LPJ dengan disokong oleh Jawatankuasa Pemandu ICT LPJ (JPICT) yang terdiri daripada: a) PPB Bhg. Khidmat Korporat & Pembangunan – Pegawai Digital (CDO) b) PPB Bahagian c) Pegawai Teknologi Maklumat - Pegawai Keselamatan ICT (ICTSO) d) Semua ketua unit e) Ahli-ahli yang dilantik Polisi ini perlu disebarkan dan dipatuhi oleh semua Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak Pengurusan Tertinggi LPJ kepada Warga LPJ, pembekal, pakar	Ketua Jabatan

5.1: POLISI KESELAMATAN MAKLUMAT *(POLICIES FOR INFORMATION SECURITY)*	
PERKARA	**PERANAN**
runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ.	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
5.2.1 KETUA JABATAN Peranan dan tanggungjawab KJ adalah seperti berikut: a) Memastikan penguatkuasaan pelaksanaan Polisi ini; b) Memastikan semua Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan d) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan e) Melantik CDO dan ICTSO.	Ketua Jabatan

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
5.2.2 KETUA PEGAWAI DIGITAL *(CDO)*	
PPB Bahagian Khidmat Korporat & Pembangunan dilantik sebagai CDO. Peranan dan tanggungjawab beliau adalah seperti berikut: a) Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan dalam Polisi ini; b) Memastikan kawalan keselamatan maklumat dalam LPJ diseragam dan diselaras dengan sebaiknya; c) Memastikan Pelan Strategik Pendigitalan LPJ mengandungi aspek keselamatan siber; dan d) Menyelaras pelan latihan dan program kesedaran keselamatan siber.	PPB Bahagian Khidmat Korporat & Pembangunan
5.2.3 PENGURUS ICT	
Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a) Memastikan Polisi Keselamatan Siber LPJ dilaksanakan dan dipatuhi di bahagian; b) Memastikan semua pengguna di LPJ mematuhi dasar, piawaian dan garis panduan keselamatan ICT, dan seterusnya melaporkan sebarang insiden	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
berkaitan keselamatan ICT; c) Mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu, dengan persetujuan ICTSO; d) Melaksanakan keperluan Polisi Keselamatan Siber dalam operasi semasa seperti berikut: i. Pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; ii. Pembelian atau peningkatan perisian dan sistem komputer; iii. Perolehan teknologi dan perkhidmatan komunikasi baru; iv. Pelantikan pembekal, perunding atau rakan usahasama; dan v. Menentukan pembekal, perunding atau rakan usahasama menjalani tapisankeselamatan selaras dengan keperluan tahap perkhidmatan. e) Memastikan bentuk ancaman keselamatan terkini dikenalpasti dan penemuan ancaman dilaporkan kepada ICTSO; f) Menyemak dan mengesahkan garis	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
panduan, prosedur dan tatacara bagi semua aplikasi yang dibangunkan di bahagian-bahagian agar mematuhi keperluan Polisi Keselamatan Siber LPJ; g) Membangun, mengkaji semula dan mengemaskini pelan kontingensi dengan mengaktifkan Pelan Pemulihan Bencana (DRP); dan h) Memastikan sistem kawalan capaian pengguna ke atas aset-aset ICT LPJ dilaksanakan.	
5.2.4 PEGAWAI KESELAMATAN ICT *(ICTSO)*	
Pegawai Teknologi Maklumat merupakan ICTSO LPJ. Peranan dan tanggungjawab ICTSO adalah seperti berikut : a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; b) Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; c) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap	Pegawai Teknologi Maklumat

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; d) Melaporkan insiden keselamatan siber kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara dan seterusnya membantu dalam penyiasatan atau pemulihan e) Melaporkan insiden kepada CDO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP); f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; g) Melaksanakan pematuhan Polisi ini oleh Warga LPJ, pembekal, pakar rundingdan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ; h) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber;dan i) Menyedia dan merangka latihan dan program kesedaran keselamatan siber.	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
j) Menjadi Pengarah Pasukan CSIRT LPJ.	
5.2.5 KETUA UNIT	
Semua Ketua Unit di LPJ berperanan dan bertanggungjawab dalam melaksanakan keperluan Polisi ini dalam operasi semasa bahagian/unit seperti yang berikut: a) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; b) Pembelian atau peningkatan perisian dan sistem komputer; c) Perolehan teknologi dan perkhidmatan komunikasi baru; d) Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan e) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa.	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
5.2.6 PENTADBIR SISTEM APLIKASI / PERKHIDMATAN DIGITAL	
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi/Perkhidmatan Digital adalah seperti berikut: a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini; c) Memantau aktiviti capaian sistem aplikasi; d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e) Menganalisis dan menyimpan rekod jejak audit; f) Menyediakan laporan mengenai aktiviti capaian secara berkala;	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
g) Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; h) Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; i) Memastikan *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi terkemaskini supayaterhindar daripada ancaman virus dan penggodam; j) Mematuhi dan melaksanakan prinsip-prinsip Polisi ini dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi; k) Memastikan *backup* sistem aplikasi dan data yang berkaitan dengannya dibuat secara berjadual; l) Menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya; m) Melaporkan kepada CSIRT LPJ jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya;	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
5.2.7 PENTADBIR TEKNIKAL	
Peranan dan tanggungjawab Pentadbir Teknikal adalah seperti berikut : a) Menyediakan khidmat sokongan teknikal ICT; b) Merancang dan melaksanakan perolehan aset ICT; c) Mengurus pendaftaran, agihan, penempatan dan pelupusan Aset ICT; d) Memastikan semua aset ICT diselenggarakan secara berkala dengan sempurna; e) Memastikan perisian antivirus dipasang pada Aset ICT; dan f) Mengurus Meja Bantuan ICT LPJ;	
5.2.8 PENTADBIR RANGKAIAN	
Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut : a) Memastikan rangkaian setempat (LAN), rangkaian luas (WAN) dan rangkaian Wireless LPJ beroperasi sepanjang masa; b) Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna;	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabildan sebarang kerosakan perkakasan sokongan rangkaian LPJ; e) Memantau penggunaan rangkaian dan melaporkan kepada CSIRT LPJ sekiranya berlaku penyalahgunaan sumber rangkaian; f) Mewartakan polisi dan garis panduan penggunaan rangkaian LPJ kepada pengguna rangkaian; g) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan luar ke dalam rangkaian LPJ secara tidak sah; h) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian.	
5.2.9 PENTADBIR LAMAN WEB/PORTAL *(WEBMASTER)*	
Peranan dan tanggungjawab pentadbir Laman Web adalah seperti berikut:	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
a) Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b) Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; d) Menghadkan capaian Pentadbir Laman Web bahagian/unit ke web server; e) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; f) Melaporkan sebarang pelanggaran keselamatan laman portal kepada CSIRT LPJ.	
5.2.10 PENTADBIR E-MEL	
Peranan dan tanggungjawab pentadbir E-Mel adalah seperti berikut: a) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Jabatan.	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar Polisi dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b) Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c) Menyimpan jejak audit selama sekurang-kurangnya enam (6) bulan di dalam pelayan e-mel ATAU tertakluk kepada kemampuan ruang storan; d) Melaksanakan jadual penstoran dan pengarkiban e-mel. Penyimpanan media storan sama ada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin bagi mengelak daripada sebarang risiko seperti kehilangan maklumat; e) Memastikan akaun e-mel pengguna sentiasa dalam keadaan baik dan berfungsi; f) Memastikan keselamatan akaun e-mel pengguna dari ancaman luar dan dalam; g) Melaksanakan penyelenggaraan ke atas sistem e-mel dengan baik dan	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
menentukan segala *patches* terkini yang disediakan oleh pihak pembekal dipasang dan berfungsi dengan sempurna; h) Memantau status storan e-mel Pengurusan Atasan LPJ dan memastikan e-mel Pengurusan Atasan LPJ sentiasa tersedia untuk transaksi e-mel; i) Memastikan semua peralatan sistem e-mel sentiasa aktif 24 x 7; j) Memastikan agar keupayaan *mail relay* hanya boleh digunakan untuk server atau aplikasi dalaman LPJ sahaja bagi tujuan keselamatan; k) Memastikan kemudahan membuat capaian e-mel melalui pelbagai media seperti telefon mudah alih disediakan kepada pengguna e-mel LPJ; dan l) Memastikan pengguna e-mel LPJ berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel LPJ dan Internet serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan melalui latihan serta promosi.	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
5.2.11 PEGAWAI ASET ICT	
Peranan dan tanggungjawab pegawai aset ICT adalah seperti berikut : a) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; b) Memastikan Aset ICT milik LPJ dilabel dan direkodkan ke dalam Sistem Pengurusan Aset; c) Memastikan Aset milik LPJ dibuat pemeriksaan berkala secara tahunan dan diselenggara sebaiknya agar dapat meningkatkan jangka hayat Aset ICT tersebut; d) Memastikan Aset ICT untuk pinjaman dan simpanan sebelum agihan diletakkan di dalam bilik stor yang mempunyai kawalan keselamatan yang terjamin; e) Memastikan Stok alat ganti Aset ICT sentiasa mencukupi dan disimpan di tempat yang selamat dan terkawal; dan f) Memastikan Aset ICT yang ingin dilupuskan dilaksanakan mengikut garis	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
panduan kawalan keselamatan bagi pelupusan data digital.	
5.2.12 PENTADBIR PUSAT DATA DAN DISASTER RECOVERY CENTER (DRC)	
Peranan dan tanggungjawab pegawai adalah seperti berikut : a) Memastikan Operasi Pusat Data dan DRC berada dalam keadaan baik 24 x 7; b) Merancang dan menyelia pelaksanaan simulasi *Disaster Recovery Plan (DRP)* LPJ; c) Pengurus operasi DRC sekiranya berlaku bencana terhadap Pusat Data LPJ; d) Memastikan Operasi Infrastruktur Virtualisasi di Pusat Data dan DRC berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; e) Memastikan Operasi *Backup / Restore* Data berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; f) Memantau Aset ICT sokongan dan Fasiliti Sokongan (*Precision Aircond,*	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
Alat Pencegah Kebakaran, Alarm, Bekalan Elektrik) di Pusat Data dan DRC bagi memastikan beroperasi lancar24 x 7; g) Menguruskan permohonan baru dan pengemaskinian server dan *Virtual Machine* bagi sistem aplikasi baru di Pusat Data dan DRC; h) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian- perisian lain di web server dan pusat data; dan i) Menguruskan Khidmat Sokongan Operasi Server dari segi Penerimaan, Penyediaan, Penyelenggaraan, Waranti, Pengeluaran dan Pelupusan.	
5.2.13 JAWATANKUASA PEMANDU ISMS	
Peranan dan tanggungjawab Jawatankuasa Pemandu ISMS adalah seperti berikut: a) Menentukan hala tuju keseluruhan pelaksanaan pensijilan ISMS LPJ yang merangkumi perancangan, pemantauan dan pengesahan terhadap perkara-perkara berikut:	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
i. Pelaksanaan pensijilan ISMS ke atas perkhidmatan Pejabat LPJ yang dikenalpasti; ii. Kelulusan ke atas dasar, objektif, dan skop pelaksanaan ISMS; iii. Penetapan kriteria penerimaan risiko, tahap risiko dan *risk treatment plan* b) Keputusan dan tindakan Mesyuarat Jawatankuasa Kerja ISMS LPJ; c) Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan LPJ yang dikenal pasti; d) Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik LPJ; e) Keperluan ISMS diterapkan dalam budaya kerja warga LPJ; f) Sumber yang diperlukan oleh pasukan pelaksana ISMS; g) Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya; h) Pencapaian sasaran ISMS seperti yang dirancang;	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
i) Arahan dan sokongan kepada pasukan ISMS LPJ bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan j) Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan. Meluluskan: a) Struktur Organisasi ISMS LPJ; b) Keperluan sumber; dan c) Pelantikan Pasukan Audit Dalam ISMS LPJ.	
5.2.14 PASUKAN CSIRT LPJ	
Peranan dan Tanggungjawab CSIRT adalah seperti berikut : a) Menerima dan mengesan aduan keselamatan siber dan menilai tahap dan jenis insiden; b) Merekodkan dan menjalankan siasatan awal insiden yang diterima; c) Menangani tindak balas (*response*) insiden keselamatan siber dan mengambil tindakan baik pulih minima; d) Menghubungi dan melaporkan insiden yang berlaku kepada NACSA MKN sama ada sebagai input atau untuk tindakan seterusnya;	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
e) Menasihatkan agensi-agensi di bawah kawalannya mengambil tindakan pemulihan dan pengukuhan; f) Menyebarkan makluman berkaitan pengukuhan keselamatan siber kepada agensi di bawah kawalannya; dan g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supayainsiden baru dapat dielakkan.	
5.2.15 PENGGUNA	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Membaca, memahami dan mematuhi Polisi ini; b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; c) Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat; d) Mematuhi prinsip-prinsip Polisi ini dan menjaga kerahsiaan maklumat LPJ;	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
e) Melaksanakan langkah-langkah perlindungan seperti berikut :- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan siber yang ditetapkan; vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan bagi setiap langkah-langkah keselamatan siber dari diketahui umum.	

5.2: PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(THE ROLE AND RESPONSIBILITY OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
f) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada Pasukan CSIRT LPJ dengan segera; g) Menghadiri program-program kesedaran mengenai keselamatan siber; dan h) Menandatangani surat akuan pematuhan Polisi Keselamatan Siber LPJ sebagaimana Lampiran 1.	

5.3 : PENGASINGAN TUGAS *(SEGREGATION OF DUTIES)*	
PERKARA	**PERANAN**
5.3.1 KETUA UNIT	
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubahsuai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;	

5.3 : PENGASINGAN TUGAS *(SEGREGATION OF DUTIES)*	
PERKARA	**PERANAN**
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; c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya;	

5.4 : TANGGUNGJAWAB PENGURUSAN (*MANAGEMENT RESPONSIBILITIES)*	
PERKARA	**PERANAN**
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubahsuai,	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

5.4 : TANGGUNGJAWAB PENGURUSAN (*MANAGEMENT RESPONSIBILITIES*)	
PERKARA	**PERANAN**
tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Pengurusan hendaklah memastikan warga kerja LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	

5.5 : HUBUNGAN DENGAN PIHAK BERKUASA (*CONTACT WITH AUTHORITIES*)	
PERKARA	**PERANAN**
5.5.1 PASUKAN CSIRT LPJ	
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab LPJ; b) mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa	

5.5 : HUBUNGAN DENGAN PIHAK BERKUASA (*CONTACT WITH AUTHORITIES*)	
PERKARA	**PERANAN**
perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan c) insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	

5.6 : HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS *(CONTACT WITH SPECIAL INTEREST GROUPS)*	
PERKARA	**PERANAN**
5.6.1 WARGA LPJ (PASUKAN PROJEK)	
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di LPJ; b) objektif keselamatan maklumat hendaklah diambil kira dalam	

5.6 : HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS *(CONTACT WITH SPECIAL INTEREST GROUPS)*	
PERKARA	**PERANAN**
pengurusan projekmerangkumi semua fasa pelaksanaan metodologi projek; c) pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; dan d) kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber LPJ.	

5.7 : ANCAMAN PERISIKAN *(THREAT INTELLIGENCE)*	
PERKARA	**PERANAN**
Teknologi Informasi dan Komunikasi (ICT) adalah serangkaian langkah dan tindakan yang diambil untuk mengesan, melindungi, dan mencegah berbagai jenis ancaman perisikan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Sistem pemantauan (*Security Monitoring*) bagi mengesan aktiviti yang mencurigakan atau ancaman perisikan	

5.7 : ANCAMAN PERISIKAN *(THREAT INTELLIGENCE)*	
PERKARA	**PERANAN**
yang mungkin terjadi di dalam rangkaian atau sistem. b) Memasang pendinding api *(Firewall)* bagi mengawal lalu lintas jaringan rangkaian daripada aktiviti yang mencurigakan. c) Setiap data yang disimpan hendaklah di enkripsi (*Encryption*) bagi melindungi data daripada dicapai oleh orang tidak sah. d) Memastikan setiap perisian yang digunakan adalah yang terkini dan sentiasa dikemaskini. e) Mengawal akses setiap pengguna aplikasi sistem mengikut skop tugas yang telah ditetapkan oleh pemilik sistem. f) Membahagikan rangkaian di dalam sesebuah organisasi kepada beberapa bahagian mengikut tingkat atau sebagainya. g) Mengkaji, menilai dan mengemaskini teknologi perkakasan atau perisian mengikut keadaan semasa.	

5.8 : KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK *(INFORMATION SECURITY IN PROJECT MANAGEMENT)*	
PERKARA	**PERANAN**
5.8.1 WARGA LPJ (PASUKAN PROJEK)	
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di LPJ; b) objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; c) pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenai pasti kawalan-kawalan yang diperlukan; dan d) kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber LPJ.	

5.9 : MAKLUMAT INVENTORI ASET DAN YANG BERKAITAN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
PERKARA	**PERANAN**
5.9.1 INVENTORI ASET (*INVENTORY OF ASSETS*)	
Memastikan semua aset ICT LPJ hendaklah disokong dan diberi perlindungan yang bersesuaian. Perkara yang perlu dipatuhi adalah seperti berikut: a) Mengenal pasti Pegawai Penerima Aset setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT; b) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkodkan dan sentiasa dikemaskini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; d) Pegawai Aset hendaklah mengesahkan penempatan aset ICT; e) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan	

5.9 : MAKLUMAT INVENTORI ASET DAN YANG BERKAITAN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
f) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	
5.9.2 PEMILIKAN ASET *(OWNERSHIP OF ASSETS)*	
Aset ICT yang diselenggara hendaklah milik LPJ. Perkara yang perlu dipatuhi oleh pemilik aset adalah seperti berikut : a) Memastikan aset ICT di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; b) Memastikan aset ICT telah dikelaskan dan dilindungi; c) Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; d) Memastikan pengendalian aset ICT dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan e) Memastikan semua jenis aset dipelihara dengan baik.	

5.9 : MAKLUMAT INVENTORI ASET DAN YANG BERKAITAN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
5.9.3 PENGGUNAAN ASET YANG DIBENARKAN *(ACCEPTABLE USE OF ASSETS)*	
Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	
5.9.4 PEMULANGAN ASET (*RETURN OF ASSETS*)	
Memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	

5.10 : MAKLUMAT PENGGUNAAN ASET YANG BOLEH DITERIMA DAN YANG BERKAITAN *(ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
PERKARA	**PERANAN**
5.10.1 PENGGUNAAN ASET YANG DIBENARKAN *(ACCEPTABLE USE OF ASSETS)*	
Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	
5.10.2 PENGENDALIAN ASET *(HANDLING OF ASSETS)*	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah	

5.10 : MAKLUMAT PENGGUNAAN ASET YANG BOLEH DITERIMA DAN YANG BERKAITAN *(ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
mengambil kira langkah-langkah keselamatan berikut : a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.	

5.11 : PEMULANGAN ASET *(RETURN OF ASSETS)*	
PERKARA	**PERANAN**
Memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	

5.12 : PENGELASAN MAKLUMAT (*CLASSIFICATION OF INFORMATION*)	
PERKARA	**PERANAN**
Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad. Selain daripada maklumat terperingkat adalah dikelaskan sebagai terbuka.	

5.13 : PELABELAN MAKLUMAT *(LABELLING OF INFORMATION)*	
PERKARA	**PERANAN**
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.	

5.14 : PEMINDAHAN DATA DAN MAKLUMAT *(INFORMATION TRANSFER)*	
PERKARA	**PERANAN**
5.14.1 : POLISI DAN PROSEDUR PEMINDAHAN DATA DAN MAKLUMAT (*INFORMATION TRANSFER POLICIES AND PROCEDURES*)	
Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; b) Terma pemindahan data, maklumat dan perisian antara LPJ dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; c) Media yang mengandungi maklumat perlu dilindungi; dan d) Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya.	Pengguna, Warga LPJ dan pembekal

5.14 : PEMINDAHAN DATA DAN MAKLUMAT (*INFORMATION TRANSFER*)	
PERKARA	**PERANAN**
5.14.2 : PERJANJIAN MENGENAI PEMINDAHAN DATA DAN MAKLUMAT (*AGREEMENTS ON INFORMATION TRANSFER*)	
LPJ perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara LPJ dengan pihak luar. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) PPB Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat LPJ; b) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat LPJ; c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan d) LPJ hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	CDO dan PPB Bahagian
5.14.3 : PESANAN ELEKTRONIK (*ELEKTRONIK MESSAGING*)	
Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya	Warga LPJ

5.14 : PEMINDAHAN DATA DAN MAKLUMAT *(INFORMATION TRANSFER)*	
PERKARA	**PERANAN**
mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti: a) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; b) Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 — Pematuhan Tatacara Penggunaan E-mel dan Internet; c) Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkah- langkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan; dan d) mana-mana undang-undang bertulis Kerajaan Persekutuan yang berkuat kuasa; Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut : a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh LPJ sahaja boleh digunakan. Penggunaan akaun milik	

5.14 : PEMINDAHAN DATA DAN MAKLUMAT *(INFORMATION TRANSFER)*	
PERKARA	**PERANAN**
orang lain atau akaun yang dikongsi bersama adalah dilarang; b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh LPJ; c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (25Mb) atau mengikut polisi yang ditetapkan agensi semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;	

5.14 : PEMINDAHAN DATA DAN MAKLUMAT *(INFORMATION TRANSFER)*	
PERKARA	**PERANAN**
h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti Yahoo Mail, Gmail, Hotmail dan sebagainya) tidak digunakan untuk tujuan rasmi; dan m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing- masing.	

5.15 : KAWALAN AKSES *(ACCESS CONTROL)*	
PERKARA	**PERANAN**
5.15.1 : POLISI KAWALAN KESELAMATAN (*ACCESS CONTROL POLICY*)	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan	

5.15 : KAWALAN AKSES *(ACCESS CONTROL)*	
PERKARA	**PERANAN**
keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu diwujudkan, didokumenkan, dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Keperluan keselamatan aplikasi; b) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; c) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; d) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; e) Pengasingan peranan kawalan capaian; f) Kebenaran rasmi permintaan akses; g) Keperluan semakan hak akses berkala; h) Pembatalan hak akses; i) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan j) Capaian *privilege*.	

5.15 : KAWALAN AKSES *(ACCESS CONTROL)*	
PERKARA	**PERANAN**
5.15.2 : KAWALAN CAPAIAN KEPADA RANGKAIAN DAN PERKHIDMATAN RANGKAIAN (*ACCESS TO NETWORK AND NETWORK SERVICES*)	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari LPJ. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Memastikan hanya pengguna yang dibenarkan sahaja boleh mendapat perkhidmatan rangkaian; b) Menempatkan, mengasingkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian LPJ, rangkaian agensi lain dan rangkaian awam; dan c) Mewujud, menguatkuasakan dan memantau mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar. d) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	

5.16 : PENDAFTARAN DAN PEMBATALAN AKAUN PENGGUNA (*USER REGISTRATION AND DE-REGISTRATION*)	
PERKARA	**PERANAN**
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi : a) Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c) Akaun pengguna yang diwujudkan pertama kali akan diberi capaian minimum yang akan ditetapkan oleh pemilik sistem; d) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik perkhidmatan digital atau aplikasi terlebih dahulu; e) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan	Semua Pengguna dan Warga LPJ

5.16 : PENDAFTARAN DAN PEMBATALAN AKAUN PENGGUNA (*USER REGISTRATION AND DE-REGISTRATION*)	
PERKARA	**PERANAN**
g) Pentadbir Sistem Aplikasi/Perkhidmatan Digital boleh membeku dan menamatkan akaun pengguna atas sebab- sebab berikut: i. Pengguna bercuti panjang / menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan	

5.17 : MAKLUMAT PENGESAHAN *(AUTHENTICATION INFORMATION)*	
PERKARA	**PERANAN**
5.17.1 PENGURUSAN MAKLUMAT PENGESAHAN RAHSIA PENGGUNA *(MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS)*	
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	ICTSO dan Pentadbir Perkhidmatan Digital /Aplikasi

5.17 : MAKLUMAT PENGESAHAN *(AUTHENTICATION INFORMATION)*	
PERKARA	**PERANAN**
5.17.2 : PENGGUNAAN MAKLUMAT PENGESAHAN RAHSIA (*USE OF SECRET AUTHENTICATION INFORMATION)*	
Peranan dan tanggungjawab pengguna adalah seperti yang berikut: a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber LPJ; b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat LPJ; d) Melaksanakan langkah-langkah perlindungan seperti yang berikut : i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran,	

5.17 : MAKLUMAT PENGESAHAN *(AUTHENTICATION INFORMATION)*	
PERKARA	**PERANAN**
penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum. e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan f) Menghadiri program-program kesedaran mengenai keselamatan siber.	
5.17.3 : PENGURUSAN KATA LALUAN *(PASSWORD MANAGEMENT)*	
Sistem pengurusan kata laluan hendaklah interaktif dan mengambil kira kualiti kata laluan yang dicipta. Pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mengikut amalan keselamatan yang baik serta prosedur yang ditetapkan oleh LPJ untuk melindungi maklumat yang digunakan untuk pengesahan identiti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;	

5.17 : MAKLUMAT PENGESAHAN *(AUTHENTICATION INFORMATION)*	
PERKARA	**PERANAN**
c) Panjang kata laluan mestilah sekurang-kurangnya LAPAN (8) AKSARA dengan gabungan antara huruf, aksara khas dan nombor (*alphanumeric*) KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; d) Kata laluan tidak boleh didedahkan dengan apa cara sekalipun; e) Kata laluan papan kekunci (*lock screen*) dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; g) Bagi sistem aplikasi, kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Bagi sistem aplikasi, had cubaan kemasukan kata laluan bagi capaian adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan dibekukan.	

5.17 : MAKLUMAT PENGESAHAN *(AUTHENTICATION INFORMATION)*	
PERKARA	**PERANAN**
Kemasukan kata laluan seterusnya hanya boleh dibuat selepas bagi tempoh masa tertentu (mengikut kesesuaian sistem) atau setelah diset semula oleh Pentadbir Sistem Aplikasi/Perkhidmatan Digital; j) Kata laluan hendaklah ditukar selepas seratus dua puluh (120) hari atau selepas tempoh masa yang bersesuaian; k) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

5.18: HAK AKSES *(ACCESS RIGHTS)*	
PERKARA	**PERANAN**
5.18.1: PERUNTUKAN AKSES PENGGUNA *(USER ACCESS PROVISIONING)*	
Satu proses untuk penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.	Pentadbir Perkhidmatan Digital/ Aplikasi
5.18.2 : KAJIAN SEMULA HAK AKSES PENGGUNA *(REVIEW OF USER ACCESS RIGHTS)*	
Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan. Pentadbir Perkhidmatan Digital /Aplikasi perlu mewujudkan Prosedur/SOP berkaitan	ICTSO dan Pentadbir Perkhidmatan Digital /Aplikasi

5.18: HAK AKSES *(ACCESS RIGHTS)*	
PERKARA	**PERANAN**
Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.	
5.18.3 : KAJIAN PEMBATALAN ATAU PELARASAN HAK AKSES (*REVIEW OR ADJUSTMENTS OF ACCESS RIGHTS*)	
Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/ dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam jabatan.	Pentadbir Perkhidmatan Digital / Aplikasi

5.19 : POLISI KESELAMATAN MAKLUMAT UNTUK HUBUNGAN PEMBEKAL (*INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS*)	
PERKARA	**PERANAN**
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset LPJ. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori; b) Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal;	PPB Bahagian, Pemilik Projek, Pembekal

5.19 : POLISI KESELAMATAN MAKLUMAT UNTUK HUBUNGAN PEMBEKAL (*INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS*)	
PERKARA	**PERANAN**
c) Mengawal dan memantau akses pembekal; d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; e) Jenis-jenis obligasi kepada pembekal; f) Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; g) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber LPJ kepada pembekal; h) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber LPJ (Lampiran 3); dan i) Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.	

5.20 : MENANGANI KESELAMATAN DALAM PERJANJIAN PEMBEKAL (*ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS)*	
PERKARA	**PERANAN**
Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan atau menyediakan	Pembekal

5.20 : MENANGANI KESELAMATAN DALAM PERJANJIAN PEMBEKAL (*ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS*)	
PERKARA	**PERANAN**
komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak LPJ selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak LPJ mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) LPJ hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan;	

5.20 : MENANGANI KESELAMATAN DALAM PERJANJIAN PEMBEKAL (*ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS*)	
PERKARA	**PERANAN**
c) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; d) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; e) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal; f) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: i. Badan penilai pihak ketiga adalah bebas dan berintegriti; ii. Badan penilai pihak ketiga adalah kompeten; iii. Kriteria penilaian; iv. Parameter pengujian; dan v. Andaian yang dibuat berkaitan dengan skop penilaian. g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan	

5.20 : MENANGANI KESELAMATAN DALAM PERJANJIAN PEMBEKAL (*ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS*)	
PERKARA	**PERANAN**
maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan LPJ; dan h) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh LPJ.	

5.21 : RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (*INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN*)	
PERKARA	**PERANAN**
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada kontraktor atau	PPB Bahagian, Pemilik Projek, Pembekal

5.21 : RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (*INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN)*	
PERKARA	**PERANAN**
pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	

5.22: MEMANTAU, MENGKAJI SEMULA DAN MENGURUSKAN PERUBAHAN PERKHIDMATAN PEMBEKAL *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)*	
PERKARA	**PERANAN**
5.22.1 : MEMANTAU DAN MENGKAJI SEMULA PERKHIDMATAN PEMBEKAL *(MONITORING AND REVIEW SUPPLIER SERVICES)*	
LPJ hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan	PPB Bahagian, Pemilik Projek, Pembekal

5.22: MEMANTAU, MENGKAJI SEMULA DAN MENGURUSKAN PERUBAHAN PERKHIDMATAN PEMBEKAL *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)*	
PERKARA	**PERANAN**
c) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	
5.22.2 : MENGURUSKAN PERUBAHAN KEPADA PERKHIDMATAN PEMBEKAL *(MANAGING CHANGES TO SUPPLIER SERVICES*)	
Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut: a) Perubahan dalam perjanjian dengan pembekal; b) Perubahan yang dilakukan oleh LPJ bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk	PPB Bahagian, Pemilik Projek, Pembekal

5.22: MEMANTAU, MENGKAJI SEMULA DAN MENGURUSKAN PERUBAHAN PERKHIDMATAN PEMBEKAL *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)*	
PERKARA	**PERANAN**
baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	

5.23 : KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	
PERKARA	**PERANAN**
Perkhidmatan awan adalah penting untuk memastikan bahawa organisasi memilih penyedia perkhidmatan awam yang mempunyai tahap keselamatan yang tinggi. Berikut adalah beberapa langkah-langkah yang diperlukan sebelum penggunaan perkhidmatan awan. a) Menetapkan skop perolehan perkhidmatan awan yang ingin dikawal. Skop ini perlu merangkumi jenis perkhidmatan awan yang diperlukan, data yang akan dipindahkan ke awan, dan syarat-syarat keselamatan yang dikehendaki. b) Melakukan penilaian risiko untuk mengenal pasti potensi ancaman dan kerentanan yang berkaitan dengan penggunaan perkhidmatan awan. Ini memungkinkan anda untuk mengenal pasti tahap risiko dan mengambil	

5.23 : KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	
PERKARA	**PERANAN**
tindakan untuk mengurangkan risiko tersebut. c) Memilih penyedia perkhidmatan awan yang mematuhi piawaian keselamatan maklumat dan memiliki rekod prestasi yang baik dalam bidang keselamatan dan privasi data. d) Membuat perjanjian perkhidmatan dengan penyedia perkhidmatan awan yang mencukupi butiran keselamatan maklumat, seperti tahap layanan, perlindungan data, pematuhan piawaian, pemisahan data, pemulihan bencana, dan peraturan pematuhan. e) Melakukan audit keselamatan secara berkala ke atas penyedia perkhidmatan awan untuk memastikan pematuhan mereka terhadap perjanjian perkhidmatan dan piawaian keselamatan maklumat. f) Memastikan bahawa penyedia perkhidmatan awan mempunyai perancangan pemulihan bencana yang kukuh untuk melindungi data organisasi dalam kejadian insiden yang merugikan. g) Menilai semula keselamatan maklumat secara berkala dan memastikan ia	

5.23 : KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	
PERKARA	**PERANAN**
selaras dengan keperluan keselamatan dan piawaian. h) Memastikan bahawa organisasi mematuhi peraturan dan perundangan yang berkaitan dengan penggunaan perkhidmatan awan, terutamanya dalam hal privasi data dan perlindungan data peribadi.	

5.24 : PELAPORAN KELEMAHAN KESELAMATAN MAKLUMAT (*REPORTING SECURITY WEAKNESSES)*	
PERKARA	**PERANAN**
Warga LPJ dan pembekal yang menggunakan sistem dan perkhidmatan maklumat LPJ dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

5.25 : PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT *(ASSESSMENT OF AND DECISION ON INFORMATION SECURITY EVENTS)*	
PERKARA	**PERANAN**
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO

5.26 : TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT (*RESPONSE TO INFORMATION SECURITY INCIDENTS)*	
PERKARA	**PERANAN**
Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT LPJ. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b) Menjalankan kajian forensik sekiranya perlu; c) Menghubungi pihak yang berkenaan dengan secepat mungkin;	ICTSO, CSIRT LPJ

5.26 : TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT (*RESPONSE TO INFORMATION SECURITY INCIDENTS*)	
PERKARA	**PERANAN**
d) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; f) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; g) Menyediakan tindakan pemulihan segera; dan h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	

5.27 : PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT *(LEARNING FROM INFORMATION SECURITY INCIDENTS)*	
PERKARA	**PERANAN**
Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan	ICTSO, CSIRT LPJ

5.27 : PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT *(LEARNING FROM INFORMATION SECURITY INCIDENTS)*	
PERKARA	**PERANAN**
untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	

5.28 : PENGUMPULAN BAHAN BUKTI *(COLLECTION OF EVIDENCE)*	
PERKARA	**PERANAN**
LPJ hendaklah menentukan prosedur untuk mengenai pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan	ICTSO, CSIRT LPJ

5.29 : KESELAMATAN MAKLUMAT SEMASA GANGGUAN *(INFORMATION SECURITY DURING DISRUPTION)*	
PERKARA	**PERANAN**
5.29.1 : PERANCANGAN KESINAMBUNGAN KESELAMATAN MAKLUMAT *(PLANNING INFORMATION SECURITY CONTINUITY)*	
LPJ hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, LPJ perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh	Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team(ERT), Critical Communication Team (CCT) LPJ

5.29 : KESELAMATAN MAKLUMAT SEMASA GANGGUAN *(INFORMATION SECURITY DURING DISRUPTION)*	
PERKARA	**PERANAN**
memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi LPJ. LPJ juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) LPJ; b) Menetapkan polisi PKP; c) Mengenal pasti perkhidmatan kritikal; d) Melaksanakan Kajian Impak Perkhidmatan (Business Impact Analysis — BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; e) Membangunkan Pelan lnduk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT. f) Melaksanakan program kesedaran dan latihan pasukan PKP dan Warga LPJ; g) Melaksanakan simulasi ke atas dokumen di para (c); dan h) Melaksanakan penyelenggaraan ke atas pelan di para (c).	

5.29 : KESELAMATAN MAKLUMAT SEMASA GANGGUAN *(INFORMATION SECURITY DURING DISRUPTION)*	
PERKARA	**PERANAN**
5.29.2 : PELAKSANAN KESINAMBUNGAN KESELAMATAN MAKLUMAT *(IMPLEMENTING INFORMATION SECURITY CONTINUITY*)	
LPJ hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal LPJ yang telah dikenal pasti berdasarkan kepada Pelan lnduk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini; b) Melaksanakan post-mortem dan mengemaskini pelan-pelan PKP; c) Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal LPJ; d) Mengemas kini struktur tadbir urus PKP LPJ jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan	Pengurusan Tertinggi LPJ, Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team(ERT), Critical Communication Team (CCT) LPJ

5.29 : KESELAMATAN MAKLUMAT SEMASA GANGGUAN *(INFORMATION SECURITY DURING DISRUPTION)*	
PERKARA	**PERANAN**
e) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.	
5.29.3 : MENENTUSAHKAN, MENGKAJI SEMULA DAN MENILAI KESINAMBUNGAN KESELAMATAN MAKLUMAT *(VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY*)	
LPJ hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.	Pengurusan Tertinggi LPJ, Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team(ERT), Critical Communication Team (CCT) LPJ, Pemilik Perkhidmatan Kritikal LPJ dalam PKP dan Warga LPJ

5.30 : KETERSEDIAAN ICT UNTUK KESINAMBUNGAN *PERKHIDMATAN (ICT READINESS FOR BUSINESS CONTINUITY)*	
PERKARA	**PERANAN**
Teknologi Maklumat dan Komunikasi (ICT) adalah aspek penting dalam memastikan kesinambungan operasi organisasi. Ini melibatkan penyediaan infrastruktur, sistem, dan perkhidmatan ICT yang boleh diakses dan	Pengurus ICT, ICTSO, Pentadbir Rangkain, Pentadbir Sistem Aplikasi

5.30 : KETERSEDIAAN ICT UNTUK KESINAMBUNGAN *PERKHIDMATAN (ICT READINESS FOR BUSINESS CONTINUITY)*	
PERKARA	**PERANAN**
berfungsi dengan baik dalam semua keadaan, termasuk semasa krisis atau gangguan. Faktor-faktor yang perlu dipertimbangkan untuk mencapai ketersediaan ICT bagi kesinambungan organisasi adalah seperti berikut : a) Organisasi perlu mempunyai perancangan strategik ICT yang jelas dan menyeluruh yang mengenal pasti keperluan teknologi bagi menjayakan strategi kesinambungan perniagaan. b) Ini termasuk menentukan sumber daya ICT yang diperlukan, tujuan pemulihan, dan kebijakan perolehan peralatan dan perkhidmatan c) Mempunyai infrastruktur ICT yang *redundant*, termasuk rangkaian, pelayan, storan data, dan sokongan kuasa yang boleh berfungsi jika ada gangguan atau kegagalan. d) Penggantian secara automatik (*failover*) dan peralatan cadangan perlu dipertimbangkan. e) Lakukan pemantauan aktif terhadap peralatan ICT untuk mengenalpasti masalah sebelum ia berlaku dan mengelakkan gangguan.	

5.30 : KETERSEDIAAN ICT UNTUK KESINAMBUNGAN *PERKHIDMATAN (ICT READINESS FOR BUSINESS CONTINUITY)*	
PERKARA	**PERANAN**
f) Pengurusan inventori peralatan, pelan pembaikan, dan pemantauan prestasi berterusan. g) Sediakan pelan pemulihan bencana ICT yang komprehensif. Ini termasuk cadangan data, pengekalkan cadangan pelayan, dan prosedur pemulihan semula aktiviti perniagaan. h) Ujian dan latihan berkala pelan pemulihan bencana. i) Pastikan akses kepada sistem dan data dikawal dengan ketat dan disemak secara berkala. Ini termasuk pengurusan identiti, pengesahihan dua faktor, dan peraturan akses yang ketat. j) Sediakan perkhidmatan pengurusan keselamatan seperti antivirus, firewall, dan pelindung kegagalan untuk menghalang ancaman keselamatan ICT. k) Amalkan pemantauan keselamatan untuk mengenalpasti dantindak balas kepada ancaman dan insiden keselamatan. l) Pastikan kakitangan tahu apa yang perlu dilakukan dalam kes insiden keselamatan.	

5.30 : KETERSEDIAAN ICT UNTUK KESINAMBUNGAN *PERKHIDMATAN (ICT READINESS FOR BUSINESS CONTINUITY)*	
PERKARA	**PERANAN**
m) Melaksanakan penyelenggaraan dan pembaikan peralatan dan sistem secara berkala untuk mengelakkan kegagalan yang tidak dijangka. n) Tetapkan jadual pembaikan berkala dan pemulihan data. o) Pantau penggunaan sumber daya ICT seperti bandwidth dan kapasiti penyimpanan untuk mengelakkan penggunaan berlebihan yang boleh menyebabkan gangguan. p) Pastikan penyedia perkhidmatan awan atau penyedia perkhidmatan lain mempunyai pelan kesinambungan perniagaan yang mencukupi yang dapat menyokong operasianda jika berlaku gangguan	

5.31 : UNDANG-UNDANG, BERKANUN, PERATURAN DAN KEPERLUAN KONTRAK *(LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS)*	
PERKARA	**PERANAN**
5.31.1 : PENGENALPASTIAN KEPERLUAN UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI *(IDENTIFICATION OF APPLICABLE LEGISLATION AND CONTRACTUAL AGREEMENT)*	
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ. Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di LPJ dan pembekal adalah seperti di Lampiran 2.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ LPJ
5.31.2 : PERATURAN KAWALAN KRIPTOGRAFI (*REGULATION OF CRYPTOGRAPHIC CONTROLS)*	
LPJ hendaklah mengguna pakai kawalan kriptografi yang mematuhi undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

5.32 : HAK HARTA INTELEK *(INTELLECTUAL PROPERTY RIGHTS)*	
PERKARA	**PERANAN**
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

5.33 : PERLINDUNGAN REKOD (*PROTECTION OF RECORDS*)	
PERKARA	**PERANAN**
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

5.34 : PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI *(PRIVACY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION)*	
PERKARA	**PERANAN**
LPJ hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

5.35 : KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI *(INDEPENDENT REVIEW OF INFORMATION SECURITY)*	
PERKARA	**PERANAN**
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	PPB Bahagian dan Pemilik Perkhidmatan

5.36 : PEMATUHAN POLISI, PERATURAN & PIAWAIAN KESELAMATAN MAKLUMAT *(COMPLIANCE WITH POLICIES, RULES AND STANDARDS FOR INFORMATION SECURITY)*	
PERKARA	**PERANAN**
5.36.1 : PEMATUHAN POLISI DAN STANDARD KESELAMATAN *(COMPLIANCE WITH SECURITY POLICIES AND STANDARDS)*	
LPJ hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi,	PPB Bahagian dan Pemilik Perkhidmatan

5.36 : PEMATUHAN POLISI, PERATURAN & PIAWAIAN KESELAMATAN MAKLUMAT *(COMPLIANCE WITH POLICIES, RULES AND STANDARDS FOR INFORMATION SECURITY)*	
PERKARA	**PERANAN**
piawaian dan keperluan teknikal yang bersesuaian.	
5.36.2 : KAJIAN SEMULA PEMATUHAN TEKNIKAL *(TECHNICAL COMPLIANCE REVIEW)*	
LPJ hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.	PPB Bahagian dan Pemilik Perkhidmatan

5.37 : PROSEDUR OPERASI YANG DIDOKUMENKAN (*DOCUMENTED OPERATING PROCEDURES*)	
PERKARA	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Semua prosedur keselamatan siber yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian serta pemprosesan maklumat, pengendalian serta	USTM, CSIRT LPJ

5.37 : PROSEDUR OPERASI YANG DIDOKUMENKAN (*DOCUMENTED OPERATING PROCEDURES*)	
PERKARA	**PERANAN**
penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	

ANNEX A **6**	**ANNEX A6 : KAWALAN SUMBER MANUSIA** ***(PEOPLE CONTROL)***

6.1 : TAPISAN KESELAMATAN *(SECURITY SCREENING)*	
PERKARA	**PERANAN**
Tapisan keselamatan hendaklah dijalankan terhadap Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b) Menjalankan tapisan keselamatan untuk Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan,	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

6.1 : TAPISAN KESELAMATAN *(SECURITY SCREENING)*	
PERKARA	**PERANAN**
peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	

6.2 : TERMA DAN SYARAT PERKHIDMATAN *(TERMS AND CONDITIONS OF EMPLOYMENT)*	
PERKARA	**PERANAN**
Persetujuan berkontrak dengan Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: a) menyatakan dengan lengkap dan jelas peranan serta tanggungjawab Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ yang terlibat dalam menjamin keselamatan aset ICT; dan b) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

6.3 : KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT (*INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING)*	
PERKARA	**PERANAN**
Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut : a) memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber LPJ, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/ fungsi/ aplikasi/ sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; b) memastikan kesedaran yang berkaitan Polisi Keselamatan Siber LPJ perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

6.3 : KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT (*INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING)*	
PERKARA	**PERANAN**
c) memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	

6.4 : PROSES TATATERTIB *(DISCIPLINARY PROCESS)*	
PERKARA	**PERANAN**
Proses tatatertib yang formal dan disampaikan kepada Warga LPJ hendaklah tersedia bagi membolehkan tindakan diambil terhadap Warga LPJ yang melakukan pelanggaran keselamatan maklumat. Perkara- perkara yang perlu dipatuhi adalah seperti yang berikut: d) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas Warga LPJ sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh LPJ; e) Warga LPJ yang melanggar polisi ini akan dikenakan tindakan tatatertertib atau	Unit Integriti

6.4 : PROSES TATATERTIB *(DISCIPLINARY PROCESS)*	
PERKARA	**PERANAN**
digantung daripada mendapat capaian kepada kemudahan ICT LPJ.	

6.5 : PENAMATAN ATAU PERTUKARAN TANGGUNGJAWAB PERKHIDMATAN (*TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES*)	
PERKARA	**PERANAN**
Warga LPJ yang telah tamat perkhidmatan/bertukar perkhidmatan perlu mematuhi perkara- perkara berikut: a) Memastikan semua aset ICT LPJ dikembalikan kepada LPJ mengikut peraturan dan/atau terma yang ditetapkan; b) Memastikan semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat dibatalkan oleh pentadbir sistem mengikut peraturan yang ditetapkan oleh LPJ. c) Maklumat rasmi LPJ dalam peranti tidak dibenarkan dibawa keluar dari LPJ. d) Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	Warga LPJ, Pentadbir Sistem

6.5 : PENAMATAN ATAU PERTUKARAN TANGGUNGJAWAB PERKHIDMATAN (*TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES*)	
PERKARA	**PERANAN**
Unit Pengurusan Sumber Manusia perlu: a) Mengemaskini semua dokumentasi berkaitan pegawai yang tamat perkhidmatan bagi memastikan kesinambungan perkhidmatan LPJ	

6.6 : PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN (*CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS*)	
PERKARA	**PERANAN**
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal;	ICTSO, BPB Bahagian, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital, Pengguna dan Pembekal

6.6 : PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN (*CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS*)	
PERKARA	**PERANAN**
b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak pembekal perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	

6.7: KERJA JAUH *(REMOTE WORKING)*	
PERKARA	**PERANAN**
6.7.1 WARGA LPJ	
Peranan dan tanggungjawab adalah seperti berikut: a) Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja.	Warga LPJ

6.8 : PELAPORAN KESELAMATAN MAKLUMAT (*INFORMATION SECURITY EVENT REPORTING)*	
PERKARA	**PERANAN**
6.8.1: PELAPORAN KEJADIAN KESELAMATAN MAKLUMAT (*REPORTING INFORMATION SECURITY EVENTS*)	
Insiden keselamatan maklumat seperti berikut hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT LPJ kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Maklumat didapati atau disyaki hilang, atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses didapati atau disyaki hilang, dicuri atau didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	ICTSO, PPB Bahagian, CSIRT LPJ

6.8 : PELAPORAN KESELAMATAN MAKLUMAT (*INFORMATION SECURITY EVENT REPORTING)*	
PERKARA	**PERANAN**
Prosedur pelaporan insiden keselamatan Siber berdasarkan : a) Surat Arahan CIO 18 Februari 2011 – Proses Kerja Pelaporan Insiden Keselamatan ICT *Computer Emergency Response Team* (CERT) LPJ. b) Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT SIRT LPJ; dan c) Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam	
6.8.2 : PELAPORAN KELEMAHAN KESELAMATAN MAKLUMAT (*REPORTING SECURITY WEAKNESSES)*	
Warga LPJ dan pembekal yang menggunakan sistem dan perkhidmatan maklumat LPJ dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

ANNEX A **7**	**ANNEX A7 : KESELAMATAN FIZIKAL DAN PERSEKITARAN (*PHYSICAL AND ENVIRONMENTAL SECURITY*)**

7.1 : PERIMETER KESELAMATAN FIZIKAL *(PHYSICAL SECURITY PARAMETER)*	
PERKARA	**PERANAN**
Ini bertujuan untuk menghalang akses tanpa kebenaran, kerosakan dan gangguan secara fizikal terhadap premis, maklumat dan Aset ICT LPJ. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;	BKP

7.1 : PERIMETER KESELAMATAN FIZIKAL *(PHYSICAL SECURITY PARAMETER)*	
PERKARA	**PERANAN**
d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau- bilau manusia dan sebarang bencana alam atau perbuatan manusia; e) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan g) Memasang alat penggera atau kamera keselamatan;	

7.2 : KAWALAN KEMASUKAN FIZIKAL (*PHYSICAL ENTRY CONTROLS)*	
PERKARA	**PERANAN**
7.2.1 : KAWALAN KEMASUKAN FIZIKAL (*PHYSICAL ENTRY CONTROLS)*	
Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis LPJ. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Setiap Warga LPJ hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas;	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

7.2 : KAWALAN KEMASUKAN FIZIKAL (*PHYSICAL ENTRY CONTROLS)*	
PERKARA	**PERANAN**
b) Semua pas keselamatan hendaklah diserahkan kembali kepada jabatan apabila pengguna bertukar, tamat perkhidmatan atau bersara; c) Setiap pelawat boleh mendapatkan Pas Keselamatan Pelawat di Lobi Bangunan Ibupejabat LPJ terlebih dahulu dan hendaklah dikembalikan semula selepas tamat lawatan; d) Kehilangan pas mestilah dilaporkan dengan segera; dan e) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan Aset ICT LPJ.	
7.2.2 : KAWASAN PENYERAHAN DAN PEMUNGGAHAN *(DELIVERY AND LOADING AREAS)*	
Titik kemasukan (*access point)* seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. LPJ hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

7.2 : KAWALAN KEMASUKAN FIZIKAL (*PHYSICAL ENTRY CONTROLS)*	
PERKARA	**PERANAN**
dimasuki oleh pihak yang tidak diberi kebenaran.	

7.3 : KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN (*SECURING OFFICES, ROOMS AND FACILITIES)*	
PERKARA	**PERANAN**
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; b) Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan c) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

7.4 : PEMANTAUAN KESELAMATAN FIZIKAL *(PHYSICAL SECURITY MONITORING)*	
PERKARA	**PERANAN**
Akses tanpa kebenaran ke kawasan fizikal terhad seperti bilik pelayan dan bilik peralatan IT boleh mengakibatkan kehilangan kerahsiaan, ketersediaan, integriti dan keselamatan aset maklumat. Berikut adalah kawalan yang boleh dilaksanakan: a) Kamera CCTV b) Pengawal keselamatan c) Penggera keselamatan untuk penceroboh d) Alat perisian untuk pengurusan keselamatan fizikal	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

7.5 : PERLINDUNGAN DARIPADA ANCAMAN LUAR DAN PERSEKITARAN (*PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS*)	
PERKARA	**PERANAN**
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. LPJ perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	Pentadbir Pusat Data dan BKP

7.6 : BEKERJA DI KAWASAN SELAMAT (*WORKING IN SECURE AREA)*	
PERKARA	**PERANAN**
Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi Warga LPJ yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis LPJ termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut: a) Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; b) Akses adalah terhad kepada Warga LPJ yang telah diberi kuasa sahaja dan dipantau pada setiap masa; c) Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai; d) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;	Pentadbir Pusat Data dan BKP

7.6 : BEKERJA DI KAWASAN SELAMAT (*WORKING IN SECURE AREA)*	
PERKARA	**PERANAN**
e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab disepanjang tempoh di lokasi berkaitan; g) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; h) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; i) Memperkukuh dinding dan siling; dan j) Mengehadkan jalan keluar masuk.	

7.7 : DASAR MEJA KOSONG DAN SKRIN KOSONG *(CLEAR DESK DAN CLEAR SCREEN)*	
PERKARA	**PERANAN**
Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

7.7 : DASAR MEJA KOSONG DAN SKRIN KOSONG *(CLEAR DESK DAN CLEAR SCREEN)*	
PERKARA	**PERANAN**
Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Menggunakan kemudahan *screen saver password* atau *logout* apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat. d) E-mel masuk dan keluar hendaklah dikawal; dan e) Menghalang penggunaan tanpa kebenaran bagi peralatan seperti mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	

7.8 : PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT *(EQUIPMENT SITTING AND PROTECTION)*	
PERKARA	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pegawai Aset ICT / Ketua Jabatan; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

7.8 : PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT *(EQUIPMENT SITTING AND PROTECTION)*	
PERKARA	**PERANAN**
g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set (Gen-Set*); j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k) Semua peralatan yang digunakan secara berterusan tanpa henti mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l) Peralatan ICT yang hendak dibawa keluar dari premis LPJ, perlulah mendapat kelulusan Pegawai Aset ICT / Ketua Jabatan dan direkodkan bagi tujuan pemantauan;	

7.8 : PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT *(EQUIPMENT SITTING AND PROTECTION)*	
PERKARA	**PERANAN**
m) Peralatan ICT yang hilang hendaklah dilaporkan kepada Pegawai Aset ICT / Ketua Jabatan dengan segera; n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset ICT / Ketua Jabatan; p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan melalui Sistem Aduan ICT: (https://portal.lpj.gov/DashboardAll.aspx?Module=Helpdesk) untuk dibaikpulih; q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan pada semua Aset ICT. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pegawai Aset ICT; t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di	

7.8 : PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT *(EQUIPMENT SITTING AND PROTECTION)*	
PERKARA	**PERANAN**
bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; u) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat; v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada LPJ; dan w) Memastikan plag dicabut daripada suis utama *(main switch)* bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya. x) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi sahaja.	

7.9 : KESELAMATAN PERALATAN DAN ASET DI LUAR PREMIS (*SECURITY OF EQUIPMENT OFF-PREMISES*)	
PERKARA	**PERANAN**
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis LPJ. Peralatan yang dibawa keluar dari premis LPJ adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Peminjam perlu bertanggungjawab terhadap keselamatan Aset ICT yang dipinjam; b) Aset ICT perlu dilindungi dan dikawal sepanjang masa; c) Penyimpanan atau penempatan Aset ICT perlu mengambil kira ciri-ciri keselamatan lokasi yang bersesuaian; dan d) Sebarang kehilangan semasa peminjaman Aset ICT tersebut perlulah dilaporkan kepada pihak Berkuasa dan kepada Pegawai Aset ICT/ Ketua Jabatan.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

7.10 : PENGURUSAN MEDIA BOLEH ALIH *(MEDIA HANDLING)*	
PERKARA	**PERANAN**
7.10.1 : PENGURUSAN MEDIA BOLEH ALIH (*MANAGEMENT OF REMOVABLE MEDIA*)	
Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh LPJ. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan e) Menyimpan semua jenis media di tempat yang selamat.	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital dan Pengguna
7.10.2 : PELUPUSAN MEDIA *(DISPOSAL OF MEDIA)*	
a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan. b) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital dan Jawatankuasa yang dilantik untuk pelupusan aset.

7.10 : PENGURUSAN MEDIA BOLEH ALIH *(MEDIA HANDLING)*	
PERKARA	**PERANAN**
terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	
7.10.3 : PEMINDAHAN MEDIA FIZIKAL *(PHYSICAL MEDIA TRANSFER)*	
a) Pemindahan media fizikal keluar premis perlu mendapat kelulusan dan mengikut kaedah pemindahan aset ICT yang ditetapkan oleh Kerajaan. b) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dipindahkan mengikut prosedur yang berkuat kuasa.	Pemilik media
7.10.4 : PENGALIHAN ASET *(REMOVAL OF ASSETS)*	
Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Aset ICT yang dibawa untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan Aset ICT: a) Aset ICT yang dibawa keluar dari premis LPJ mestilah mendapat kelulusan Pegawai Aset ICT atau Ketua Bahagian/Unit atau Ketua Jabatan dan tertakluk kepada tujuan yang dibenarkan;	Pengguna, Pegawai Aset

7.10 : PENGURUSAN MEDIA BOLEH ALIH *(MEDIA HANDLING)*	
PERKARA	**PERANAN**
b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan;	

7.11 : UTILITI SOKONGAN (*SUPPORTING UTILITIES*)	
PERKARA	**PERANAN**
Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT

7.12 : KESELAMATAN KABEL (*CABLING SECURITY*)	
PERKARA	**PERANAN**
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:	USTM, BKP

7.12 : KESELAMATAN KABEL (*CABLING SECURITY*)	
PERKARA	**PERANAN**
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*, dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

7.13 : PENYELENGGARAAN PERKAKASAN *(EQUIPMENT MAINTENANCE)*	
PERKARA	**PERANAN**
Peralatan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti yang berterusan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan oleh pengeluar;	Pegawai Aset ICT dan Unit Operasi, USTM, LPJ

7.13 : PENYELENGGARAAN PERKAKASAN *(EQUIPMENT MAINTENANCE)*	
PERKARA	**PERANAN**
b) Memastikan perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pegawai Aset ICT / Ketua Jabatan.	

7.14 : PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*	
PERKARA	**PERANAN**
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh LPJ dan ditempatkan di bahagian/ unit.	Pegawai Aset ICT, dan Warga LPJ

7.14 : PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*	
PERKARA	**PERANAN**
Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (*overwrite*) sebelum dilupuskan atau diguna semula. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan di LPJ. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu dengan cara yang selamat; b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d) Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;	

7.14 : PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*	
PERKARA	**PERANAN**
e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri- ciri keselamatan bagi menjamin keselamatan peralatan tersebut; f) Pegawai Aset ICT bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset; g) Pelupusan peralatan ICT LPJ hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan h) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk, motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana	

7.14 : PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*	
PERKARA	**PERANAN**
peralatan yang berkaitan ke lokasi berlainan tanpa kebenaran; iii. Memindah keluar dari Agensi atau Jabatan bagi mana-mana peralatan ICT milik LPJ yang hendak dilupuskan tanpa kebenaran; iv. Melupuskan sendiri peralatan ICT LPJ kerana kerja-kerja pelupusan di bawah tanggungjawab LPJ; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumb drive* atau *external hard disk* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	

ANNEX A **8**	**ANNEX A8 : KAWALAN TEKNOLOGI** ***(TECHNOLOGICAL CONTROL)***

8.1 : PERANTI AKHIR PENGGUNA *(USER END POINT DEVICES)*	
PERKARA	**PERANAN**
8.1.1 : POLISI PERANTI MUDAH ALIH *(MOBILE DEVICE POLICY)*	
8.1.1.1 BAHAGIAN TEKNOLOGI MAKLUMAT, LPJ (USTM)	
Peranan dan tanggungjawab adalah seperti berikut: a) Membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih.	
8.1.1.2 JPICT	
Peranan dan tanggungjawab adalah seperti berikut: a) Meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada Warga LPJ.	
8.1.1.3 WARGA LPJ	
Perkara-perkara yang perlu dipatuhi: a) pendaftaran ke atas peralatan mudah alih; b) keperluan ke atas perlindungan secara fizikal;	

8.1 : PERANTI AKHIR PENGGUNA *(USER END POINT DEVICES)*	
PERKARA	**PERANAN**
c) kawalan ke atas pemasangan perisian peralatan mudah alih; d) kawalan ke atas Versi dan *patches* perisian; e) sekatan ke atas akses perkhidmatan maklumat secara dalam talian; f) kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan g) peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.	
8.1.2 : PERALATAN PENGGUNA TANPA KAWALAN *(UNATTENDED USER EQUIPMENT)*	
Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: a) Tamatkan sesi aktif apabila selesai tugas; b) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan c) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

8.2 : PERUNTUKAN HAK AKSES ISTIMEWA *(MANAGEMENT OF PRIVILEGED ACCESS RIGHTS)*	
PERKARA	**PERANAN**
Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada Borang Permohonan Akses Sistem Aplikasi.	Pentadbir Perkhidmatan Digital/ Aplikasi

8.3 : SEKATAN AKSES MAKLUMAT *(INFORMATION ACCESS RESTRICTION)*	
PERKARA	**PERANAN**
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pengguna, Pentadbir Perkhidmatan Digital /Aplikasi, ICTSO

8.4 : KAWALAN AKSES KEPADA KOD SUMBER PROGRAM *(ACCESS CONTROL TO PROGRAM SOURCE CODE)*	
PERKARA	**PERANAN**
Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber;	Pengarah Projek, Pengurus Projek dan Pentadbir Perkhidmatan Digital/ Aplikasi

8.4 : KAWALAN AKSES KEPADA KOD SUMBER PROGRAM *(ACCESS CONTROL TO PROGRAM SOURCE CODE)*	
PERKARA	**PERANAN**
b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan c) Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik LPJ.	

8.5 : PROSEDUR LOG MASUK YANG SELAMAT *(SECURE LOG-ON PROCEDURE)*	
PERKARA	**PERANAN**
Kawalan capaian terhadap sistem aplikasi perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut: a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; b) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem; c) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin;	Pentadbir Perkhidmatan Digital/ Aplikasi, ICTSO

8.5 : PROSEDUR LOG MASUK YANG SELAMAT *(SECURE LOG-ON PROCEDURE)*	
PERKARA	**PERANAN**
d) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	

8.6 : PENGURUSAN CAPACITY (*CAPACITY MANAGEMENT)*	
PERKARA	**PERANAN**
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. 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	Pemilik Sistem Aplikasi/Perkhidmatan Digital, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.6 : PENGURUSAN CAPACITY (*CAPACITY MANAGEMENT)*	
PERKARA	**PERANAN**
b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	

8.7 : KAWALAN DARIPADA PERISIAN HASAD (*CONTROLS AGAINST MALWARE*)	
PERKARA	**PERANAN**
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan malware hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut : a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti Antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS), *Content filtering* dan *Web Application Firewall*	USTM, Pengguna

8.7 : KAWALAN DARIPADA PERISIAN HASAD (*CONTROLS AGAINST MALWARE*)	
PERKARA	**PERANAN**
(WAF) serta mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa; c) Memastikan perisian antivirus mempunyai pengurusan berpusat bagi memudahkan penetapan polisi dan penyediaan laporan jika berlaku *virus outbreak* dalam rangkaian; d) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya serta dilaksanakan secara berkala; e) Mengemas kini antivirus dengan signature/*pattern* terkini; f) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; g) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;	

8.7 : KAWALAN DARIPADA PERISIAN HASAD (*CONTROLS AGAINST MALWARE*)	
PERKARA	**PERANAN**
h) 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; i) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan j) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	

8.8 : PENGURUSAN KELEMAHAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)*	
PERKARA	**PERANAN**
8.8.1 : PENGURUSAN KERENTANAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)*	
Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital dan CSIRT LPJ

8.8 : PENGURUSAN KELEMAHAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)*	
PERKARA	**PERANAN**
dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; b) Menganalisis tahap risiko kerentanan; dan c) Mengambil tindakan pengolahan dan kawalan risiko.	
8.8.2 : KAJIAN SEMULA PEMATUHAN TEKNIKAL *(TECHNICAL COMPLIANCE REVIEW)*	
LPJ hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.	BPB Bahagian dan Pemilik Perkhidmatan

8.9 : PENGURUSAN KONFIGURASI *(CONFIGURATION MANAGEMENT)*	
PERKARA	**PERANAN**
Pengurusan konfigurasi ialah bahagian penting dalam operasi pengurusan aset organisasi yang lebih luas. Konfigurasi adalah kunci dalam memastikan rangkaian bukan sahaja beroperasi sebagaimana mestinya, tetapi juga dalam melindungi peranti daripada perubahan yang tidak dibenarkan atau pindaan yang salah di pihak kakitangan penyelenggaraan dan/atau vendor a) Cuba untuk menggunakan panduan khusus vendor dan/atau sumber terbuka yang tersedia secara umum tentang cara terbaik untuk mengkonfigurasi aset perkakasan dan perisian. b) Memenuhi keperluan keselamatan minimum untuk peranti, aplikasi atau sistem yang sesuai untuknya. c) Bekerja selaras dengan usaha keselamatan maklumat organisasi yang lebih luas, termasuk semua kawalan ISO yang berkaitan. d) Perlu diingat keperluan perniagaan unik organisasi - terutamanya dalam hal konfigurasi keselamatan - termasuk kebolehlaksanaan untuk menggunakan atau mengurus templat pada bila-bila masa.	ICTSO dan Pentadbir Sistem Aplikasi

8.9 : PENGURUSAN KONFIGURASI *(CONFIGURATION MANAGEMENT)*	
PERKARA	**PERANAN**
e) Disemak pada selang masa yang sesuai untuk memenuhi kemas kini sistem dan/atau perkakasan, atau sebarang ancaman keselamatan yang berlaku.	

8.10 : PEMADAMAN MAKLUMAT *(INFORMATION DELETION)*	
PERKARA	**PERANAN**
Organisasi harus sedar tentang kewajipan mereka untuk memadamkan data yang disimpan pada pelayan dalaman, pemacu keras, tatasusunan dan pemacu USB apabila ia tidak lagi diperlukan dengan: a) Pilih kaedah pemadaman yang sesuai yang mematuhi mana-mana undang-undang atau peraturan sedia ada. Pilihan termasuk pemadaman biasa, tulis ganti atau penghapusan dikodkan. b) Rekodkan hasil penyingkiran untuk rujukan masa hadapan. c) Pastikan bahawa, apabila menggunakan vendor pemadaman khusus, organisasi memperoleh bukti yang mencukupi (biasanya melalui dokumentasi) bahawa pemadaman telah dilakukan. d) Organisasi harus menyatakan dengan tepat keperluan mereka apabila	ICTSO dan Pentadbir Sistem Aplikasi

8.10 : PEMADAMAN MAKLUMAT *(INFORMATION DELETION)*	
PERKARA	**PERANAN**
menggunakan vendor pihak ketiga, termasuk kaedah pemadaman dan jangka masa, dan harus menjamin bahawa aktiviti pemadaman dimasukkan dalam kontrak yang mengikat.	

8.11 : DATA MASKING *(DATA MASKING)*	
PERKARA	**PERANAN**
Apabila menggunakan salah satu daripada teknik ini, organisasi harus mempertimbangkan: a) Tahap penyamaran dan/atau penyamaran yang diperlukan, berbanding dengan sifat data. b) Cara data bertopeng sedang diakses. c) Sebarang perjanjian mengikat yang menyekat penggunaan data untuk disembunyikan. d) Mengekalkan data bertopeng berasingan daripada mana-mana jenis data lain, untuk mengelakkan subjek data dikenal pasti dengan mudah. e) Meneliti data yang diterima, dan bagaimana ia telah diberikan kepada mana-mana sumber dalaman atau luaran.	ICTSO, Pentadbir Rangkaian

8.12 : PENCEGAHAN KEBOCORAN DATA *(DATA LEAKAGE PREVENTION)*	
PERKARA	**PERANAN**
Kebocoran data sukar untuk dihapuskan sepenuhnya. Walau bagaimanapun, untuk meminimumkan risiko yang unik untuk operasi mereka, organisasi harus: a) Klasifikasikan data selaras dengan piawaian industri yang diiktiraf (PII, data komersial, maklumat produk), untuk menetapkan tahap risiko yang berbeza-beza di seluruh bahagian. b) Memantau dengan teliti saluran data yang diketahui yang banyak digunakan dan terdedah kepada kebocoran (cth. e-mel, pemindahan fail dalaman dan luaran, peranti USB). c) Hadkan keupayaan pengguna untuk menyalin dan menampal data (jika berkenaan) ke dan dari platform dan sistem tertentu. d) Kebenaran daripada pemilik data sebelum sebarang pemindahan data dilaksanakan. e) Pertimbangkan untuk mengurus atau menghalang pengguna daripada mengambil tangkapan skrin atau mengambil gambar monitor yang memaparkan jenis data yang dilindungi. f) Sulitkan sandaran yang mengandungi maklumat sensitif.	ICTSO, Pentadbir Rangkaian

8.12 : PENCEGAHAN KEBOCORAN DATA *(DATA LEAKAGE PREVENTION)*	
PERKARA	**PERANAN**
g) Merangka langkah keselamatan pintu masuk dan langkah pencegahan kebocoran yang melindungi daripada faktor luaran seperti (tetapi tidak terhad kepada) pengintipan industri, sabotaj, gangguan komersial dan/atau kecurian IP. h) Memastikan perisian operating sistem dan antivirus sentiasa dikemaskini.	

8.13 : SANDARAN MAKLUMAT *(INFORMATION BACKUP)*	
PERKARA	**PERANAN**
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi	USTM

8.13 : SANDARAN MAKLUMAT *(INFORMATION BACKUP)*	
PERKARA	**PERANAN**
sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana. d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, minqquan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi *backup*; dan e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan (*off-site*) dan selamat.	

8.14 : PELAKSANAN KESINAMBUNGAN KESELAMATAN MAKLUMAT *(IMPLEMENTING INFORMATION SECURITY CONTINUITY)*	
PERKARA	**PERANAN**
LPJ hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal LPJ yang telah dikenal pasti berdasarkan kepada Pelan lnduk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini; b) Melaksanakan post-mortem dan mengemaskini pelan-pelan PKP; c) Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal LPJ; d) Mengemas kini struktur tadbir urus PKP LPJ jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan e) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan	Pengurusan Tertinggi LPJ, Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team(ERT), Critical Communication Team (CCT) LPJ

8.14 : PELAKSANAN KESINAMBUNGAN KESELAMATAN MAKLUMAT *(IMPLEMENTING INFORMATION SECURITY CONTINUITY)*	
PERKARA	**PERANAN**
peranan dan tanggungjawab dalam melaksana PKP.	

8.15 : PENGELOGAN DAN PEMANTAUAN (*LOGGING AND MONITORING*)	
PERKARA	**PERANAN**
8.15.1 : PENGELOGAN KEJADIAN (*EVENT LOGGING*)	
Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.15 : PENGELOGAN DAN PEMANTAUAN (*LOGGING AND MONITORING*)	
PERKARA	**PERANAN**
fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut : a) fail log sistem pengoperasian; b) fail log servis (web, e-mel); c) fail log aplikasi (*audit trail*); dan d) fail log rangkaian (*switch, firewall*, IPS) Pentadbir Sistem Aplikasi/Perkhidmatan Digital hendaklah melaksanakan perkara-perkara berikut: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada CSIRT LPJ.	
8.15.2 : PERLINDUNGAN MAKLUMAT LOG (*PROTECTION OF LOG INFORMATION)*	
Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.15 : PENGELOGAN DAN PEMANTAUAN (*LOGGING AND MONITORING*)	
PERKARA	**PERANAN**
8.15.3 : LOG PENTADBIR DAN PENGENDALI (*ADMINISTRATOR AND OPERATOR LOGS*)	
Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap. a) Memantau penggunaan kemudahan memproses maklumat secara berkala; b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu; c) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; d) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; e) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada Pasukan CSIRT LPJ.	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital dan CSIRT LPJ

8.16 : AKTIVITI PEMANTAUAN *(MONITORING ACTIVITIES)*	
PERKARA	PERANAN
Organisasi hendaklah memasukkan perkara berikut dalam operasi pemantauan mereka: a) Kedua-dua trafik rangkaian masuk dan keluar, termasuk data ke dan dari aplikasi b) Akses kepada platform kritikal organisasi, termasuk (tetapi tidak terhad kepada Sistem, Pelayan, Perkakasan rangkaian) c) Sistem pemantauan itu sendiri d) Fail konfigurasi e) Log peristiwa daripada peralatan keselamatan dan platform perisian f) Semakan kod yang memastikan mana-mana program boleh digunakan adalah dibenarkan dan bebas daripada ancaman. g) Pengiraan, penyimpanan dan penggunaan sumber rangkaian	ICTSO, Pentadbir Rangkaian

8.17 : PENYERAGAMAN JAM (*CLOCK SYNHRONISATION)*	
PERKARA	**PERANAN**
Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.	Pentadbir Pusat Data, Pentadbir Rangkaian

8.17 : PENYERAGAMAN JAM (*CLOCK SYNHRONISATION)*	
PERKARA	**PERANAN**
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam LPJ atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM).	

8.18 : PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA *(USE OF PRIVILEGEDUTILITY PROGRAMS)*	
PERKARA	**PERANAN**
Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem	Pentadbir Perkhidmatan Digital/ Aplikasi

8.19 : PEMASANGAN PERISIAN PADA SISTEM OPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)*	
PERKARA	**PERANAN**
8.19.1 : POLISI KESELAMATAN MAKLUMAT (*POLICIES FOR INFORMATION SECURITY*)	
Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut:	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.19 : PEMASANGAN PERISIAN PADA SISTEM OPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)*	
PERKARA	**PERANAN**
a) Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.	
8.19.2 : SEKATAN KE ATAS PEMASANGAN PERISIAN *(RESTRICTION ON SOFTWARE INSTALLATION)*	
Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ. b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital, Warga LPJ, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LPJ

8.19 : PEMASANGAN PERISIAN PADA SISTEM OPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)*	
PERKARA	**PERANAN**
c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	

8.20 : KAWALAN RANGKAIAN (*NETWORK CONTROL*)	
PERKARA	**PERANAN**
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;	Pentadbir Rangkaian

8.20 : KAWALAN RANGKAIAN (*NETWORK CONTROL*)	
PERKARA	**PERANAN**
d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e) Firewall hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian; f) Semua trafik keluar dan masuk dalam rangkaian LPJ hendaklah melalui firewall di bawah kawalan LPJ; g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h) Memasang perisian *Intrusion Prevention System* (IPS) atau *Web Application Firewall* (WAF) mengikut kesesuaian bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat di dalam rangkaian LPJ; i) Memasang Web Content Filtering untuk menyekat aktiviti Web Surfing yang dilarang semasa waktu kerja; j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan LPJ adalah tidak dibenarkan; k) Semua pengguna hanya dibenarkan menggunakan rangkaian LPJ sahaja dan	

8.20 : KAWALAN RANGKAIAN (*NETWORK CONTROL*)	
PERKARA	**PERANAN**
penggunaan rangkaian lain seperti UNIFI perlu mendapatkan kebenaran atas sebab tertentu dan penggunaannya perlulah di bawah seliaan serta pemantauan ketua bahagian/unit masing-masing; l) Sebarang penggunaan rangkaian komunikasi daripada agensi lain (contoh : EGNet, NRENet) perlulah mendapat khidmat nasihat daripada pentadbir rangkaian terlebih dahulu dan pelaksanaan secara berpusat perlulah menjadi keutamaan; m) Kemudahan rangkaian tanpa wayar (wireless) perlu dipantau dan dipastikan kawalan keselamatan serta dikawal penggunaanya; n) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi Service Level Assurance (SLA) yang telah ditetapkan; o) Menempatkan atau memasang antara muka (interfaces) yang bersesuaian di antara rangkaian LPJ, rangkaian agensi lain dan rangkaian awam; p) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna	

8.20 : KAWALAN RANGKAIAN (*NETWORK CONTROL*)	
PERKARA	**PERANAN**
dan peralatan yang menepati kesesuaian penggunaannya; q) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; r) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; s) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan rangkaian LPJ; dan t) Mewujud dan melaksana kawalan pengalihan laluan (routing control) bagi memastikan pematuhan terhadap peraturan LPJ.	

8.21 : KAWALAN CAPAIAN INTERNET (*INTERNET ACCESS CONTROL)*	
PERKARA	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Penggunaan Internet di dalam rangkaian LPJ hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk	Warga LPJ

8.21 : KAWALAN CAPAIAN INTERNET (*INTERNET ACCESS CONTROL)*	
PERKARA	**PERANAN**
tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian rangkaian LPJ; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidt*h) yang maksimum dan lebih berkesan; d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pentadbir Rangkaian berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya setelah mendapat maklumat dari Ketua Jabatan; e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Bahagian/Unit/Jabatan/ pegawai yang diberi kuasa;	

8.21 : KAWALAN CAPAIAN INTERNET (*INTERNET ACCESS CONTROL)*	
PERKARA	**PERANAN**
f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian/Unit/Jabatan/ pegawai yang diberi kuasa sebelum dimuat naik ke Internet; h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh LPJ; j) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut : i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks	

8.21 : KAWALAN CAPAIAN INTERNET (*INTERNET ACCESS CONTROL)*	
PERKARA	**PERANAN**
ucapan atau bahan- bahan yang mengandungi unsur-unsur lucah.	

8.22: KESELAMATAN PERKHIDMATAN RANGKAIAN (*SECURITY OF NETWORK SERVICES*)	
PERKARA	**PERANAN**
Pengurusan bagi semua perkhidmatan rangkaian (*inhouse atau outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	ICTSO, BPB Bahagian, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital, Pembekal

8.23 : TAPISAN LAMAN WEB *(WEB FILTERING)*	
PERKARA	**PERANAN**
Organisasi harus mewujudkan dan melaksanakan kawalan yang diperlukan untuk menghalang pekerja daripada mengakses laman web luaran yang mungkin mengandungi virus, bahan yang tidak selamat data atau jenis maklumat haram yang lain dengan: a) Laman web dengan fungsi muat naik maklumat. Akses hendaklah tertakluk kepada kebenaran dan hanya boleh diberikan atas sebab yang sah. Pekeliling	ICTSO, Pengurus ICT, Pentadbir Rangkaian

8.23 : TAPISAN LAMAN WEB *(WEB FILTERING)*	
PERKARA	**PERANAN**
Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 atau pekeliling- peliling semasa. b) Laman web yang diketahui atau disyaki mengandungi bahan berniat jahat, seperti laman web dengan kandungan perisian yang tidak selamat. c) Pelayan perintah dan kawalan. d) Laman web berniat jahat yang diperoleh daripada scammer. e) Laman web yang mengedarkan kandungan dan bahan yang menyalahi undang-undang.	

8.24 : PENGGUNAAN KRIPTOGRFI *(USE OF CRYPTOGRAPHY)*	
PERKARA	**PERANAN**
8.24.1 : POLISI PENGGUNAAN KAWALAN KRIPTOGRAFI (*POLICY ON THE USE OF CYPTOGRAPHY CONTROL)*	
Kriptografi merangkumi kaedah-kaedah seperti yang berikut: a) Enkripsi - Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*). b) Tandatangan Digital - Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah	Pengarah Projek

8.24 : PENGGUNAAN KRIPTOGRFI *(USE OF CRYPTOGRAPHY)*	
PERKARA	**PERANAN**
menggunakan tandatangan digital mengikut keperluan pelaksanaan.	
8.24.2 : PENGURUSAN KUNCI AWAM (*PUBLIC KEY MANAGEMENT*)	
Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam *(Public Key Infrastructure)* PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Warga LPJ dan USTM

8.25 : DASAR PEMBANGUNAN SELAMAT (*SECURE DEVELOPMENT POLICY)*	
PERKARA	**PERANAN**
Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Keselamatan persekitaran pembangunan; b) Keselamatan pangkalan data; c) Keperluan keselamatan dalam fasa reka bentuk; d) Keperluan *check point* keselamatan dalam carta perbatuan projek;	ICTSO, BPB Bahagian, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.25 : DASAR PEMBANGUNAN SELAMAT (*SECURE DEVELOPMENT POLICY)*	
PERKARA	**PERANAN**
e) Keperluan pengetahuan ke atas keselamatan aplikasi; f) Keselamatan dalam kawalan versi; dan g) Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	

8.26 : KEPERLUAN KESELAMATAN PERMOHONAN *(APPLICATION SECURITY REQUIREMENTS)*	
PERKARA	**PERANAN**
8.26.1 : MELINDUNGI PERKHIDMATAN APLIKASI DALAM RANGKAIAN AWAM (*SECURING APPLICATION SERVICES ON PUBLIC NETWORKS)*	
Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi LPJ. Contoh perkhidmatan sumber luaran ialah: i. Perisian sebagai satu perkhidmatan;	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.26 : KEPERLUAN KESELAMATAN PERMOHONAN *(APPLICATION SECURITY REQUIREMENTS)*	
PERKARA	**PERANAN**
ii. platform sebagai satu perkhidmatan; iii. Infrastruktur sebagai satu perkhidmatan; iv. Storan pengkomputeran awan; dan v. Pemantauan keselamatan. b) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; c) Tahap kerahsiaan bagi mengenai pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*); d) proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; e) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan f) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	

8.26 : KEPERLUAN KESELAMATAN PERMOHONAN *(APPLICATION SECURITY REQUIREMENTS)*	
PERKARA	**PERANAN**
8.26.2 : MELINDUNGI TRANSAKSI PERKHIDMATAN APLIKASI (*PROTECTING APPLICATION SERVICES TRANSACTIONS*)	
Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; b) Memastikan semua aspek transaksi dipatuhi: i. maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; ii. mengekalkan kerahsiaan maklumat; iii. mengekalkan privasi pihak yang terlibat; dan iv. protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. c) Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.	ICTSO, BPB Bahagian, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.27: PRINSIP KEJURUTERAAN SISTEM YANG SELAMAT (*SECURE SYSTEM ENGINEERING PRINCIPLES*)	
PERKARA	**PERANAN**
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation (IV&V)* sektor awam yang terkini.	BPB Bahagian, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.28 : PENGEKODAN SELAMAT *(SECURE CODING)*	
PERKARA	**PERANAN**
Amalan dan prosedur pengekodan yang selamat hendaklah mengambil kira perkara berikut untuk proses pengekodan: a) Prinsip pengekodan perisian yang selamat harus disesuaikan dengan setiap bahasa pengaturcaraan dan teknik yang digunakan. b) Penggunaan teknik dan kaedah pengaturcaraan selamat seperti pembangunan yang hendak dilakukan	Pengurus ICT,ICTSO,Pentadbir Sistem Aplikasi

8.28 : PENGEKODAN SELAMAT *(SECURE CODING)*	
PERKARA	**PERANAN**
hendaklah dibuat pengujian dan pengaturcaraan pasangan. c) Penggunaan kaedah pengaturcaraan yang berstruktur. d) Dokumentasi kod yang betul dan penyingkiran kecacatan kod. e) Larangan ke atas penggunaan kaedah pengekodan perisian yang tidak selamat seperti sampel kod yang tidak diluluskan atau kata laluan berkod keras. f) Kod yang digunakan hendaklah sentiasa dikemaskini mengikut keadaan keselamatan semasa.	

8.29 : UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*	
PERKARA	**PERANAN**
8.29.1 : PENGUJIAN KESELAMATAN SISTEM (SYSTEM SECURITY TESTING)	
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;	ICTSO, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.29 : UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*	
PERKARA	**PERANAN**
b) Membuat semakan pengesahan di dalam aplikasi untuk mengenai pasti kesilapan maklumat; dan c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	
8.29.2 : PENGUJIAN PENERIMAAN SISTEM *(SYSTEM ACCEPTING TESTING)*	
Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; b) pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat dan kepatuhan kepada Polisi Pembangunan Selamat; c) penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan	ICTSO, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital, Pengguna

8.29 : UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*	
PERKARA	**PERANAN**
d) pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan *(vulnerability scanner*).	

8.30 : DASAR PEMBANGUNAN SELAMAT (*SECURE DEVELOPMENT POLICY)*	
PERKARA	**PERANAN**
Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Keselamatan persekitaran pembangunan; b) Keselamatan pangkalan data; c) Keperluan keselamatan dalam fasa reka bentuk; d) Keperluan *check point* keselamatan dalam carta perbatuan projek; e) Keperluan pengetahuan ke atas keselamatan aplikasi; f) Keselamatan dalam kawalan versi; dan g) Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk	ICTSO, BPB Bahagian, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.30 : DASAR PEMBANGUNAN SELAMAT (*SECURE DEVELOPMENT POLICY)*	
PERKARA	**PERANAN**
mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	

8.31: PERSEKITARAN PEMBANGUNAN PERISIAN, PENGUJIAN DAN PENGELUARAN *(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENT)*	
PERKARA	**PERANAN**
8.31.1 : PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN OPERASI *(SEPARATION OF DEVELOPMENT, TEST AND OPERATIONAL FACILITIES)*	
Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*); dan b) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.31: PERSEKITARAN PEMBANGUNAN PERISIAN, PENGUJIAN DAN PENGELUARAN *(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENT)*	
PERKARA	**PERANAN**
8.31.2 : PERSEKITARAN PEMBANGUNAN SELAMAT *(SECURE DEVELOPMENT ENVIRONMENT)*	
Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. LPJ perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; e) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	BPB Bahagian, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.32 : PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*	
PERKARA	PERANAN
8.32.1 : PENGURUSAN PERUBAHAN (CHANGE MANAGEMENT)	
Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) 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 ditetapkan; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya	USTM

8.32 : PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*	
PERKARA	PERANAN
ralat sama ada secara sengaja atau pun tidak.	
8.32.2 : PROSEDUR KAWALAN PERUBAHAN SISTEM *(SYSTEM CHANGE CONTROL PROCEDURES)*	
Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara- perkara yang perlu dipatuhi adalah seperti berikut : a) perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b) aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;	BPB Bahagian, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.32 : PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*	
PERKARA	PERANAN
d) Keperluan dan kesesuaian perubahan terhadap sistem pengoperasian dan perisian sokongan perlu dikaji terlebih dahulu. e) Sebarang perubahan sistem pengoperasian dan perisian sokongan perlu diuji dahulu di dalam *development server* sebelum dipasang di dalam server sebenar. f) Akses kepada kod sumber *(source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan g) Menghalang sebarang peluang untuk membocorkan maklumat.	
8.32.3 : KAJIAN SEMULA TEKNIKAL BAGI APLIKASI SELEPAS PERUBAHAN PLATFORM OPERASI *(TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES)*	
Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi	Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.32 : PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*	
PERKARA	PERANAN
membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan c) Memastikan perubahan yang sesuai dibuat kepada PKP LPJ dan Pelan Pemulihan Bencana Sistem yang berkaitan berdasarkan Pelan Pengurusan Keselamatan Maklumat (ISMP) sistem tersebut.	
8.32.4 : SEKATAN KE ATAS PERUBAHAN DALAM PAKEJ PERISIAN *(RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES)*	
Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	BPB Bahagian, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

8.33 : PERLINDUNGAN DATA UJIAN *(PROTECTION OF TEST DATA)*	
PERKARA	**PERANAN**
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan	ICTSO, Pentadbir Sistem Aplikasi/ Perkhidmatan Digital, Pengguna

8.33 : PERLINDUNGAN DATA UJIAN (*PROTECTION OF TEST DATA)*	
PERKARA	**PERANAN**
untuk menyalin data sebenar ke persekitaran pengujian; c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan d) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	

8.34 : KAWALAN AUDIT SISTEM MAKLUMAT *(INFORMATION SYSTEMS AUDIIT CONTROLS)*	
PERKARA	PERANAN
Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perniagaan.	ICTSO dan Pentadbir Sistem Aplikasi/ Perkhidmatan Digital

LAMPIRAN 1 : SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER LPJ

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER LPJ

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian/Unit/Syarikat : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

Tandatangan : .....

Tarikh : .....

Pengesahan Ketua Jabatan

.....
( )
Pengurus Besar
Lembaga Pelabuhan Johor

Polisi Keselamatan Siber Lembaga Pelabuhan Johor (PKS LPJ) versi 1.0 ini hendaklah dibaca bersama dengan akta, warta Kerajaan, pekeliling, surat pekeliling dan peraturan yang berkaitan dan sedang berkuatkuasa seperti berikut :

1. Akta 88 - Akta Rahsia Rasmi 1972;
2. Akta 332 - Akta Hak Cipta (Pindaan) Tahun 1997;
3. Akta 562 - Akta Tandatangan Digital 1997;
4. Akta 563 - Akta Jenayah Komputer 1997;
5. Akta 588 - Akta Komunikasi dan Multimedia 1998;
6. Akta 629 - Akta Arkib Negara 2003;
7. Akta 680 - Akta Aktiviti Kerajaan Elektronik 2007;
8. Akta 854 - Akta Keselamatan Siber 2024
9. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Polisi Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan yang bertarikh 1 Oktober 2000;
10. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 28 November 2003;
11. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005;
12. 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;
13. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan MelElektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

14. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

15. Pekeliling 1PP AM 2 : Tatacara Pengurusan Aset Alih Kerajaan (2.1 – 2.7)

16. Perintah-Perintah Am;

17. Arahan Perbendaharaan;

18. Warta Kerajaan P.U.(A)377. [Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.]

19. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

20. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.

21. Surat Arahan CIO 18 Februari 2011 – Proses Kerja Pelaporan Insiden Keselamatan ICT *Computer Emergency Response Team* (CERT) LPJ.

22. Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 — Pematuhan Tatacara Penggunaan E-mel dan Internet;

23. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) V1.0 MAMPU (April 2016)

24. Arahan Keselamatan (Semakan dan Pindaan 2017);

25. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam yang bertarikh 1 Ogos 2022;

26. Surat Pekeliling Am Bilangan 4 Tahun 2022 – Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam bertarikh 9 Disember 2022; dan

27. Surat Pekeliling Am Bilangan 3 Tahun 2024 – Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024.

PERAKUAN UNTUK DITANDATANGANI BERKENAAN
DENGAN AKTA RAHSIA RASMI 1972 DAN POLISI KESELAMATAN SIBER LPJ

NAMA PROJEK :

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkah laku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi sesuatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya perolehi adalah milik LPJ dan tidak akan membocorkan, menyiarkan atau menyampaikan,sama ada secara lisan atau dengan bertulisan atau secara media elektronik, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipanrasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis pihak berkuasa yang berkenaan.

Saya juga turut tertakluk di bawah Polisi Keselamatan Siber LPJ terkini berkenaan Perkara : Keselamatan Maklumat Dalam Hubungan Pembekal. Selain itu, saya juga telah membaca dan faham serta akan mematuhi polisi laindi dalam Polisi Keselamatan Siber LPJ yang berhubungkait dengan urusan ini.

Saya juga dengan ini mewakili

.....

mengakui bahawa semua maklumat yang dinyatakan seperti di **Lampiran A** adalah terlibat secara langsung bagi sebarang urusan yang memerlukan pematuhan akta dan Polisi Keselamatan Siber LPJ seperti semua keterangan

perenggan di atas. Oleh itu, sesiapa yang tiada dalam senarai **Lampiran A** tersebut tidak dibenarkan terlibat secara langsung bagi sebarang urusan melibatkan peruntukan Akta Rahsia Rasmi 1972.

*** Sila lengkapkan dengan tulisan HURUF BESAR**

Tandatangan	:	.....
Nama	:	.....
No. Kad Pengenalan	:	.....
Jawatan	:	.....
Jabatan/Syarikat	:	.....
Tarikh	:	.....
Alamat Jabatan/Syarikat	:	.....
		.....

Disaksikan oleh	:	.....
Nama	:	.....
No. Kad Pengenalan	:	.....
Jawatan	:	.....
Jabatan/Syarikat	:	.....
Tarikh	:	.....
Cop Jabatan/Syarikat	:	.....
		.....

LAMPIRAN A

SENARAI KAKITANGAN JABATAN / SYARIKAT YANG TERLIBAT DALAM URUSAN ANTARA JABATAN / SYARIKAT .....

DENGAN .....

*** Sila lengkapkan dengan tulisan HURUF BESAR**

BIL	NAMA & JABATAN / SYARIKAT	JAWATAN	NO KAD PENGENALAN

POLISI KESELAMATAN SIBER

LEMBAGA PELABUHAN JOHOR

www.lpj.gov.my