POLISI KESELAMATAN SIBER LHDNM

VERSI 1.1

KELULUSAN DOKUMEN

Bagi pihak Lembaga Hasil Dalam Negeri Malaysia:		
Disediakan Oleh	:	 .....
Nama	:	Ts. Muhammad Zawawi Bin Yusof
Jawatan	:	Pegawai Keselamatan ICT
Tarikh	:	14 /02/ 2025
Disemak Oleh	:	 .....
Nama	:	Ts. Ahmad Sauqi Bin Ishak
Jawatan	:	Ketua Pegawai Digital
Tarikh	:	17 / 2 / 2025
Disahkan Oleh	:	 .....
Nama	:	Khairul Halimin Bin Abdul Halim
Jawatan	:	Pengerusi Jawatankuasa Keselamatan ICT LHDNM
Tarikh	:	03/03/2025
Diluluskan Oleh	:	 .....
Nama	:	Datuk Dr. Abu Tariq Bin Jamaluddin
Jawatan	:	Ketua Pegawai Eksekutif / Ketua Pengarah Hasil Dalam Negeri
Tarikh	:	12/3/25

REKOD PINDAAN

Tarikh	Versi	Maklumat Pindaan	Tindakan
12/03/2025	1.0	Dokumen asal	Jeffrizal Abu Jaapar
08/01/2026	1.1	Pindaan : i. Rujukan Surat Pekeliling Am Bilangan 6 Tahun 2005 kepada Surat Pekeliling Am Bilangan 3 Tahun 2024 ii. Jabatan/Bahagian/Negeri/Lokaliti/ Cawangan Siasatan kepada Sektor/Jabatan/Cawangan Khas/ HASiL Negeri iii. Penambahan sub-perkara Kajian Semula Hak Capaian Pengguna di bawah perkara Kawalan Akses dan Pengurusan Identiti	Kamarul Fauzi Ahmad

ISI KANDUNGAN

GLOSARI / TERMA RUJUKAN

Antivirus	Perisian yang mengimbas virus pada media storan termasuk disket,cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dari sebarang ancaman virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat serta 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	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
Bahagian Pembangunan dan Pengurusan Fasiliti	Pihak yang bertanggungjawab dalam menguruskan infrastruktur pada setiap premis LHDNM.
Bahagian Keselamatan	Pihak yang bertanggungjawab ke atas keselamatan fizikal dan persekitaran LHDNM.
CSIRT LHDNM	Organisasi yang ditubuhkan untuk membantu LHDNM mengurus pengendalian insiden keselamatan ICT.
CCTV	*Closed-Circuit Television System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CDO	*Chief Digital Officer* (Ketua Pegawai Digital) Pegawai yang bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di LHDNM
CIA	*Confidentiality, Integrity, Availability*
Denial of service	Halangan pemberian perkhidmatan
Downloading	Aktiviti muat-turun sesuatu perisian
Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirimsupaya tidak difahami oleh orang lain kecuali penerima yang sah

Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft / *espionage*) dan penipuan (hoaxes)
Hard disk	Cakera keras Digunakan untuk menyimpan data dan boleh diakses dengan lebih pantas
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain
ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
ICTSO	*ICT Security Officer* (Pegawai Keselamatan ICT) Pegawai yang bertanggungjawab terhadap aspek yang berkaitan ICT serta perkhidmatan sistem maklumat dalam menyokong arah tuju LHDNM
Insiden Keselamatan	Musibah *(*adverse event) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat kepada pelayan (server) atau komputer lain
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian tersebut agar sentiasa berasingan
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan yang hanya boleh dicapai oleh pegawai dan kakitangan dan mereka yang diberi kebenaran sahaja
ISDN	*Integrated Services Digital Network* Menggunakan isyarat digital pada talian telefon analog sedia ada

Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindakbalas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan
ISMS	*Information Security Management System* Sistem Pengurusan Keselamatan Maklumat
Jawatankuasa Pelupusan	Pihak yang bertanggungjawab ke atas keseluruhan proses pelupusan aset ICT LHDNM
Kawalan Akses	Mengawal akses kepada identiti dan data untuk memastikan hanya individu yang diberi kuasa sahaja yang boleh mengakses maklumat identiti
Koordinator PKP	Pihak yang bertanggungjawab untuk melaksanakan proses kesinambungan perkhidmatan untuk meminimakan impak dan pemulihan dari bencana sehingga ke tahap toleransi LHDNM sekiranya terdapat gangguan kepada fungsi melalui kombinasi kawalan pencegahan dan pemulihan
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer
Lock	Mengunci komputer
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya
Mobile Code	Perisian kod yang melakukan penghantaran dari satu komputer kepada komputer yang lain dan kemudian melaksanakannya secara automatik dan fungsi yang khusus tanpa interaksi oleh pengguna

MODEM	*Modulator Demodulator* Peranti yang boleh menukar *strim bit digital* ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer
MOF	*Ministry of Finance* (Kementerian Kewangan Malaysia)
NACSA	*National Cyber Security Agency* (Agensi Keselamatan Siber Negara)
NC4	National Cyber Coodination & Command Center
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan
Pegawai Aset	Pegawai yang bertanggungjawab ke atas semua peralatan ICT LHDNM termasuk merekodkan butir-butir aset ICT LHDNM, pelupusan dan mengemaskini rekod pelupusan aset ICT LHDNM
Pentadbir Keselamatan ICT	Semua Pegawai di Seksyen Keselamatan ICT
Pentadbir Rangkaian ICT	Semua Pegawai Pengurusan Rangkaian dan Telekomunikasi di Jabatan Digital
Pentadbir Sistem ICT	Semua Pegawai Jabatan Digital yang melaksana tugas-tugas teknikal dan bertanggungjawab dalam menguruskan perisian dan perkakasan ICT LHDNM termasuk operasi sistem dan pusat data LHDNM
Pentadbir Sistem Operasi	Semua Pegawai yang dilantik bagi pengurusan ID pengguna (Capaian Pengguna)
Pengguna	Pekerja LHDNM bertaraf tetap, sementara, kontrak dan sambilan
Pengurus ICT	Semua Pengarah Bahagian dan Pengarah Seksyen di Jabatan Digital adalah merupakan Pengurus ICT
Penilaian Risiko	Menilai risiko yang mungkin timbul akibat ancaman pintar dan menentukan langkah-langkah mitigasi yang sesuai

Penyelaras ICT	Pegawai yang dilantik oleh Pengarah Jabatan / Bahagian / Negeri / Cawangan / Cawangan Siasatan masing-masing untuk menguruskan perkara-perkara yang berkaitan dengan ICT di pejabat berkenaan
Pemilik Sistem ICT	Pihak yang mengurus, mentadbir dan menjaga setiap operasi sistem maklumat dan aplikasi ICT LHDNM
Pemilik Sumber Maklumat	Pihak yang berhak dan bertanggungjawab ke atas maklumat yang disimpan
Pihak Ketiga	Pembekal, kontraktor, pakar runding dan pihak-pihak yang membekalkan perkhidmatan kepada LHDNM dan yang menggunakan aset ICT LHDNM
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet
Screen saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu
Server	Pelayan komputer
Service Account	Akaun capaian sistem atau *server* tempatan yang diwujudkan secara eksklusif untuk kegunaan mesin / server / komputer bagi melaksanakan tugasan berjadual, fungsi sandaran dan fungsi-fungsi khas seperti pengawalan gugusan, imbangan beban, pangkalan data dan fungsi-fungsi lain yang berkaitan
Source code	Kod Sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia
Switch	Suis merupakan gabungan hab yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access / Collision Detection* (CSMA / CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif peribadi dan atas sebab tertentu

Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi
WAN	*Wide Area Network* Rangkaian komputer yang merangkumi kawasan yang luas
Warga Hasil	Semua pegawai dan staf LHDNM yang dilantik untuk sesuatu jawatan sama ada tetap, sambilan, sementara atau kontrak yang berkhidmat di LHDNM
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel
PII	*Personal Identifiable Information* Maklumat peribadi yang dapat dikenalpasti

PENGENALAN

Polisi Keselamatan Siber Lembaga Hasil Dalam Negeri Malaysia (PKS LHDNM) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam sebarang urusan yang melibatkan penggunaan aset ICT LHDNM. Polisi ini menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan masing-masing dalam usaha untuk melindungi aset ICT LHDNM.

OBJEKTIF

PKS LHDNM diwujudkan untuk menjamin kesinambungan urusan LHDNM dengan meminimumkan kesan insiden yang boleh menjejaskan keselamatan aset ICT.

Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi LHDNM. Ini boleh dicapai dengan memberi perlindungan ke atas semua aset ICT LHDNM.

Objektif utama PKS LHDNM adalah seperti berikut:

a) Memastikan kelancaran operasi LHDNM dan meminimumkan kerosakan atau kemusnahan;

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

c) Mencegah penyalahgunaan aset ICT LHDNM; dan

d) Mencegah kecurian aset ICT LHDNM.

PERNYATAAN POLISI

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

Keselamatan siber bermaksud keadaan di mana segala urusan menyedia dan membekal perkhidmatan berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan siber berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan siber iaitu:

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan daripada capaian tanpa kuasa yang sah;

b) Menjamin setiap maklumat adalah tepat dan sempurna;

c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

d) Memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

PKS LHDNM merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat di atas dan kebolehsediaannya kepada semua pengguna yang dibenarkan.

CIRI–CIRI KESELAMATAN MAKLUMAT

Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a) Kerahsiaan

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

b) Integriti

Data dan maklumat hendaklah tepat, lengkap dan terkini. Ia hanya boleh diubah dengan cara yang dibenarkan;

c) Tidak Boleh Disangkal

Punca data dan maklumat hendaklah daripada sumber yang sah dan tidak boleh disangkal;

d) Kesahihan

Data dan maklumat hendaklah dijamin kesahihannya; dan

e) Ketersediaan

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

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

SKOP

Aset ICT LHDNM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat, manusia dan premis. PKS LHDNM menetapkan keperluan-keperluan asas berikut:

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

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

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

a) Perkakasan

Perkakasan adalah semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan LHDNM. Contohnya seperti komputer, pelayan, peralatan komunikasi dan sebagainya;

b) Perisian

Perisian adalah aturcara, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contohnya seperti perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada LHDNM;

c) Perkhidmatan

Perkhidmatan adalah perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contohnya adalah seperti berikut :

I. Perkhidmatan rangkaian seperti LAN dan WAN;

II. Sistem halangan akses seperti sistem kad akses; dan

III. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin dan sistem pencegah kebakaran.

d) Data atau Maklumat

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

e) Manusia

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

f) Premis Komputer dan Komunikasi

Premis komputer dan komunikasi adalah semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) hingga (e) di atas.

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

PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS LHDNM dan perlu dipatuhi adalah seperti berikut:

a) Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut;

b) Hak akses minimum

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

c) Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

I. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

II. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

III. Menentukan maklumat sedia untuk digunakan;

IV. Menjaga kerahsiaan kata laluan;

V. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

VI. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

VII. Menjaga kerahsiaan langkah-langkah keselamatan aset ICT daripada diketahui umum.

d) Pengasingan

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

e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan supaya dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f) Pematuhan

PKS LHDNM hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran yang boleh membawa ancaman kepada keselamatan aset ICT;

g) Pemulihan

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

h) Saling bergantung

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

PENILAIAN RISIKO KESELAMATAN ASET ICT

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

LHDNM hendaklah melaksanakan penilaian risiko keselamatan aset ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan aset ICT, seterusnya mengambil tindakan susulan dan / atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan aset ICT berdasarkan penemuan penilaian risiko.

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

LHDNM bertanggungjawab melaksanakan dan menguruskan risiko keselamatan aset ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 3 Tahun 2024 : Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

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

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

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

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

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

BIDANG 1 : KAWALAN ORGANISASI

ID	KETERANGAN	PERANAN
1.1 Polisi Keselamatan Maklumat		
1.1.1	**Pelaksanaan Polisi** Pelaksanaan polisi ini akan dijalankan oleh Ketua Pegawai Eksekutif / Ketua Pengarah Hasil Dalam Negeri (CEO) dibantu oleh Jawatankuasa Keselamatan ICT (JKES ICT) LHDNM.	CEO
1.1.2	**Penyebaran Polisi** Polisi ini perlu disebarkan kepada semua pengguna ICT LHDNM termasuk pegawai dan kakitangan, pembekal, kontraktor, pakar runding dan semua pihak yang berurusan dengan aset ICT LHDNM.	ICTSO
1.1.3	**Penyenggaraan Polisi** Polisi Keselamatan Siber LHDNM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berkaitan dengan penyenggaraan Polisi Keselamatan Siber LHDNM : (a) Kenalpasti dan tentukan perubahan yang diperlukan; (b) Kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan JKES ICT LHDNM;	ICTSO JKES ICT

ID	KETERANGAN	PERANAN
	(c) Maklumkan kepada semua pengguna aset ICT LHDNM perubahan yang telah dipersetujui oleh JKES ICT LHDNM; dan (d) Polisi ini hendaklah dikaji semula sekurang-kurangnya lima (5) tahun sekali atau mengikut keperluan semasa.	
1.1.4	**Pengecualian Polisi** Polisi Keselamatan Siber LHDNM adalah terpakai kepada semua pengguna ICT LHDNM dan tiada pengecualian diberikan.	Warga Hasil Pihak Ketiga
1.2 Peranan dan Tanggungjawab Keselamatan Maklumat		
1.2.1	**Peranan dan Tanggungjawab Keselamatan Maklumat** **I. Ketua Pegawai Eksekutif / Ketua Pengarah Hasil Dalam Negeri (CEO)** Peranan dan tanggungjawab Ketua Pegawai Eksekutif / Ketua Pengarah Hasil Dalam Negeri adalah seperti berikut : (a) Memastikan semua pengguna memahami peruntukan -peruntukan di bawah Polisi Keselamatan Siber LHDNM; (b) Memastikan semua pengguna mematuhi Polisi Keselamatan Siber LHDNM; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan	CEO JKES ICT LHDNM CDO ICTSO CSIRT LHDNM Pengurus ICT Pentadbir Keselamatan ICT Pentadbir Rangkaian ICT Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	perlindungan keselamatan adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi Keselamatan Siber LHDNM; (e) Memastikan perkara-perkara berkaitan dengan Keselamatan ICT LHDNM dibincangkan didalam mesyuarat JKES ICT LHDNM; (f) Melantik ahli Jawatankuasa JKES ICT LHDNM; (g) Meluluskan dokumen Polisi Keselamatan Siber LHDNM untuk dikuatkuasakan; dan/atau (h) Memutuskan tindakan yang perlu diambil terhadap sebarang insiden keselamatan ICT. **II. Jawatankuasa Keselamatan ICT LHDNM (JKES ICT LHDNM)** JKES ICT LHDNM adalah jawatankuasa yang bertanggungjawab ke atas keselamatan ICT. Jawatankuasa ini berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT LHDNM. Jawatankuasa ini juga akan bermesyuarat berdasarkan keperluan dari semasa ke semasa.	Pentadbir Sistem Operasi Penyelaras ICT Warga Hasil

ID	KETERANGAN	PERANAN
	Keanggotaan JKES ICT LHDNM adalah seperti berikut : **Pengerusi** : Timbalan Ketua Pegawai Eksekutif (Pengurusan) **Timbalan Pengerusi (Pengerusi Ganti)** : Timbalan Ketua Pegawai Eksekutif (Operasi Percukaian) **Urusetia** : Pengarah Seksyen Seksyen Strategik ICT **Anggota / ahli** : i. Pengarah Sektor Operasi Cukai ii. Pengarah Sektor Pematuhan Cukai iii. Pengarah Sektor Modal Insan iv. Pengarah Jabatan Undang-Undang v. Pengarah Jabatan Integriti Dan Pengurusan Risiko vi. Pengarah Jabatan Logistik Korporat vii. Pengarah Jabatan Digital (JD)	

ID	KETERANGAN	PERANAN
	viii. Pegawai Keselamatan ICT (ICTSO) ix. Pengarah Bahagian Aplikasi Korporat, JD x. Pengarah Bahagian Aplikasi Selain Korporat, JD xi. Pengarah Bahagian Operasi ICT, JD **Bidang kuasa:** (a) Memperakukan dokumen Polisi Keselamatan Siber LHDNM untuk kelulusan Ketua Pegawai Eksekutif / Ketua Pengarah Hasil Dalam Negeri; (b) Memantau tahap pematuhan keselamatan ICT; (c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus LHDNM yang mematuhi keperluan Polisi Keselamatan Siber LHDNM; (d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (e) Memastikan Polisi Keselamatan Siber LHDNM selaras dengan dasar-dasar ICT Kerajaan;	

ID	KETERANGAN	PERANAN
	(f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (g) Membincang tindakan yang melibatkan pelanggaran Polisi Keselamatan Siber LHDNM; dan (h) Memperakukan dan mengesyorkan tindakan yang perlu diambil mengenai sebarang insiden keselamatan ICT. III. **Ketua Pegawai Digital (CDO)** Peranan dan tanggungjawab CDO adalah seperti berikut : (a) Membantu Timbalan Ketua Pengarah (Operasi Percukaian) dan menasihati Ketua Pegawai Eksekutif / Ketua Pengarah Hasil Dalam Negeri dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan keselamatan ICT LHDNM; (c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan Polisi Keselamatan Siber LHDNM, pengurusan risiko dan pengauditan; dan (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT LHDNM.	

ID	KETERANGAN	PERANAN
	IV. Pegawai Keselamatan ICT (ICTSO) Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Mengurus keseluruhan aturcara keselamatan ICT LHDNM; (b) Menguatkuasakan pelaksanaan Polisi Keselamatan Siber LHDNM; (c) Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber LHDNM kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber LHDNM; (e) Menjalankan pengurusan risiko ICT; (f) Menjalankan audit ICT, membuat kajian semula dan merumus tindak balas ke atas penemuan audit serta menyediakan laporan kepada JKES ICT; (g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (h) Melaporkan insiden keselamatan ICT kepada Incident Response Team (IRT), National Cyber Coordination & Command Center (NC4), Agensi Keselamatan Cyber Negara (NACSA) dan	

ID	KETERANGAN	PERANAN
	memaklumkannya kepada CDO dan JKES ICT LHDNM; (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; (j) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Polisi Keselamatan Siber LHDNM kepada JKES ICT LHDNM; (k) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; (l) Bertanggungjawab melaporkan sebarang keperluan mesyuarat JKES ICT LHDNM kepada urusetia JKES ICT LHDNM; (m) Mengambil maklum mengenai perkembangan teknologi terkini yang berkaitan dengan keselamatan ICT dan mencadangkan penggunaannya kepada JKES ICT LHDNM; (n) Memastikan perolehan, pembangunan, penambahbaikan dan penyenggaraan sistem mengambil kira aspek keselamatan ICT.	

ID	KETERANGAN	PERANAN
	V. Pasukan Tindak Balas Insiden Keselamatan Siber / Cyber Security Incident Response Team (CSIRT) LHDNM Peranan dan tanggungjawab CSIRT LHDNM adalah seperti berikut : (a) Memantau, mengesan insiden, menerima, dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber. (b) Merekod dan menjalankan siasatan awal terhadap insiden yang diterima. (c) Melaksanakan pengurusan dan pengendalian insiden keselamatan siber serta mengambil tindakan awal pemulihan. (d) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan. (e) Melaporkan insiden keselamatan siber kepada agensi yang menyelianya (sekiranya ada) dan NC4. (f) Menasihati agensi di bawah seliaannya mengambil tindakan pemulihan dan pengukuhan.	

ID	KETERANGAN	PERANAN
	(g) Menyebarkan makluman/amaran berkaitan insiden kepada agensi lain di bawah seliaanya. Menyelianya (sekiranya ada) dan NC4. (h) Memastikan fail log disimpan sekurang-kurangnya enam bulan di tempat yang selamat. **VI. Pengurus ICT** Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut : (a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan LHDNM; (b) Menentukan kawalan akses semua pengguna terhadap aset ICT LHDNM; (c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT LHDNM. **VII. Pentadbir Keselamatan ICT** Peranan dan tanggungjawab Pentadbir Keselamatan ICT adalah seperti berikut : (a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber LHDNM;	

ID	KETERANGAN	PERANAN
	(b) Memastikan pengurusan keselamatan aset ICT dilaksanakan dengan sempurna; (c) Bertanggungjawab ke atas operasi komponen-komponen keselamatan ICT seperti sistem-sistem termasuklah peralatanperalatan Keselamatan ICT LHDNM; (d) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pegawai dan kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (e) Menentukan ketepatan dan kesempurnaan konfigurasi komponen-komponen keselamatan ICT serta perkhidmatan berdasarkan keperluan Pemilik Sumber Maklumat serta pengguna bersesuaian dengan peruntukan Polisi Keselamatan Siber LHDNM; (f) Memantau aktiviti capaian harian pengguna; (g) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau	

ID	KETERANGAN	PERANAN
	memberhentikannya dengan serta merta; (h) Menyimpan dan menganalisis rekod jejak audit; (i) Mengambil tindakan penambahbaikan ke atas konfigurasi serta pemulihan perkhidmatan terhadap komponen-komponen keselamatan ICT; (j) Menyediakan laporan aktiviti capaian berdasarkan keselamatan ICT kepada Pemilik Sistem ICT secara berkala; dan (k) Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT Security Posture Assessment (SPA) serta penilaian risiko keselamatan maklumat. **VIII. Pentadbir Rangkaian ICT** Peranan dan tanggungjawab Pentadbir Rangkaian ICT adalah seperti berikut: (a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber LHDNM; (b) Memantau penggunaan rangkaian ICT LHDNM; (c) Menyediakan laporan aktiviti rangkaian; (d) Memastikan pengurusan rangkaian adalah bersesuaian dengan keperluan	

ID	KETERANGAN	PERANAN
	keselamatan ICT serta dilaksanakan dengan sempurna; (e) Menentukan ketepatan dan kesempurnaan penyediaan perkhidmatan rangkaian berdasarkan keperluan Pemilik Sumber Maklumat bersesuaian dengan peruntukan Polisi Keselamatan Siber LHDNM; (f) Memantau aktiviti capaian harian pengguna; (g) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (h) Menyimpan dan menganalisis rekod jejak audit; (i) Mengambil tindakan penambahbaikan ke atas konfigurasi serta pemulihan perkhidmatan terhadap komponen-komponen rangkaian; dan (j) Menyediakan laporan aktiviti capaian rangkaian kepada Pemilik Sumber Maklumat secara berkala. **IX. Pentadbir Sistem ICT** Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut :	

ID	KETERANGAN	PERANAN
	(a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber LHDNM; (b) Bertanggungjawab ke atas sistem-sistem dan pengoperasian Pusat Data LHDNM; (c) Memastikan pengurusan sistem dan pengoperasian Pusat Data adalah bersesuaian dengan keperluan keselamatan ICT serta dilaksanakan dengan sempurna; (d) Mengambil tindakan yang bersesuaian dengan segera ke atas sistem-sistem apabila dimaklumkan mengenai pegawai dan kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (e) Menentukan ketepatan dan kesempurnaan sesuatu tahap perkhidmatan berdasarkan keperluan Pemilik Sumber Maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber LHDNM; (f) Memantau aktiviti capaian harian sistem aplikasi pengguna; (g) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;	

ID	KETERANGAN	PERANAN
	(h) Menyimpan dan menganalisis rekod jejak audit; (i) Mengambil tindakan penambahbaikan ke atas konfigurasi serta pemulihan perkhidmatan terhadap sistem-sistem dan pengoperasian Pusat Data; dan (j) Menyediakan laporan aktiviti capaian sistem-sistem kepada Pemilik Maklumat secara berkala. **X. Pentadbir Sistem Operasi** Peranan dan tanggungjawab Pentadbir Sistem Operasi adalah : (a) Mendaftar ID Pengguna baru / tambahan untuk sistem-sistem aplikasi LHDNM sebaik sahaja menerima permohonan secara bertulis atau e-mel dari Pejabat; (b) Memberi peranan kepada pengguna dan menyenggara ID Pengguna serta bertanggungjawab ke atas sistem-sistem aplikasi LHDNM; (c) Menetapkan dasar peruntukan ID Pengguna dan katalaluan dari semasa ke semasa; (d) Mengawal dan menyimpan rekod ID Pengguna; dan (e) Menerima cadangan sistem aplikasi yang dibangunkan atau ditingkatkan sendiri oleh pejabat untuk kelulusan.	

ID	KETERANGAN	PERANAN
	XI. Penyelaras ICT Peranan dan tanggungjawab Penyelaras ICT adalah seperti berikut: (a) Menyelaras aktiviti ICT di peringkat Sektor / Jabatan / Cawangan Khas / HASiL Negeri; (b) Menyelaras aktiviti ICT di antara Sektor / Jabatan / Cawangan Khas / HASiL Negeri dengan Jabatan Digital; (c) Memberikan makluman yang bersesuaian dengan segera kepada Pentadbir Keselamatan ICT, Pentadbir Rangkaian ICT dan Pentadbir Sistem ICT apabila mana-mana pegawai dan kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (d) Menentukan ketepatan dan kesempurnaan sesuatu tahap perkhidmatan berdasarkan keperluan Pemilik Sumber Maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber LHDNM; (e) Membantu memantau aktiviti capaian harian pengguna; dan (f) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran	

ID	KETERANGAN	PERANAN
	dan bertindak untuk membatalkan atau memberhentikannya dengan serta merta. Laporan hendaklah segera dibuat kepada ICTSO, Pentadbir Keselamatan ICT, Pentadbir Rangkaian ICT, Pentadbir Sistem ICT serta Ketua Perkhidmatan. **XII. Warga Hasil** Peranan dan tanggungjawab Warga Hasil adalah seperti berikut: (a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber LHDNM; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Perlu lulus tapisan keselamatan; (d) Melaksanakan prinsip-prinsip Polisi Keselamatan Siber LHDNM dan menjaga kerahsiaan maklumat LHDNM; (e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan (f) Mengikuti program-program kesedaran mengenai keselamatan ICT; (g) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber LHDNM sebagaimana **Lampiran 1A**.	

ID	KETERANGAN	PERANAN
1.3 Pengasingan Tugas		
1.3.1	**Pengasingan Tugas** Pengasingan tugas dan bidang tanggungjawab dilaksanakan bagi mengurangkan peluang pengubahsuaian data dan maklumat tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi adalah termasuk: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, menghapus, mengemaskini, mengubah dan mengesahkan maklumat hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*.	CDO ICTSO Pengurus ICT Pemilik Sistem ICT Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
1.4 Tanggungjawab Pengurusan		
1.4.1	**Tanggungjawab Pengurusan** Pengurusan hendaklah memastikan Warga Hasil, pembekal, pakar runding dan Pihak Ketiga yang mempunyai urusan dengan perkhidmatan ICT LHDNM supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	Pengarah Bahagian Ketua Unit
1.5 Hubungan dengan Pihak Berkuasa		
1.5.1	**Hubungan dengan Pihak Berkuasa** Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab LHDNM; (b) Mewujud dan mengemaskini prosedur / senarai pihak berkuasa perundangan / pihak yang perlu dihubungi semasa kecemasan. Pihak berkuasa 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	CDO ICTSO CSIRT LHDNM

ID	KETERANGAN	PERANAN
	(c) Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	
1.6 Hubungan dengan Kumpulan Berkepentingan yang Khusus		
1.6.1	**Hubungan dengan Kumpulan Berkepentingan yang Khusus** Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau pun forum bagi : (a) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; (b) Memastikan pemahaman tentang persekitaran keselamatan maklumat adalah terkini; (c) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; (d) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan (e) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Warga Hasil (Mengikut Bidang Kepakaran)

ID	KETERANGAN	PERANAN
1.7 Perisikan Ancaman		
1.7.1	**Perisikan Ancaman** Polisi berkaitan perisikan ancaman di Malaysia biasanya merangkumi beberapa aspek penting untuk melindungi sistem dan data daripada ancaman yang semakin canggih. Berikut adalah beberapa elemen utama yang sering dimasukkan dalam Polisi Keselamatan Siber : (a) Penilaian Risiko: Menilai risiko yang mungkin timbul akibat perisikan ancaman dan menentukan langkah-langkah mitigasi yang sesuai; (b) Pengurusan Keselamatan: Menetapkan struktur organisasi dan tanggungjawab untuk mengurus keselamatan ICT, termasuk peranan Ketua Pegawai Digital (CDO) dan Pegawai Keselamatan ICT (ICTSO); (c) Kawalan Akses: Mengawal akses kepada sistem dan data untuk memastikan hanya individu yang diberi kuasa sahaja yang boleh mengakses maklumat sensitive; (d) Kesedaran dan Latihan: Melaksanakan program kesedaran dan latihan untuk memastikan semua pegawai dan kakitangan memahami ancaman pintar dan cara-cara untuk menghadapinya;	CDO CSIRT LHDNM ICTSO

ID	KETERANGAN	PERANAN
	(e) Pemantauan dan Pengesanan: Menggunakan teknologi untuk memantau dan mengesan aktiviti mencurigakan dalam rangkaian ICT; (f) Tindak Balas Insiden: Menyediakan prosedur untuk bertindak balas terhadap insiden keselamatan dengan cepat dan berkesan.	
1.8 Keselamatan Maklumat dalam Pengurusan Projek		
1.8.1	**Keselamatan Maklumat dalam Pengurusan 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 LHDNM; (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 mengenal pasti kawalan-kawalan yang diperlukan; (d) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang	Warga Hasil (Pasukan Projek)

ID	KETERANGAN	PERANAN
	terkandung dalam polisi keselamatan siber LHDNM; dan (e) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.	
1.9 Inventori Maklumat dan Aset Lain yang Berkaitan		
1.9.1	**Inventori Maklumat dan Aset Lain yang Berkaitan** Inventori maklumat dan aset lain yang berkaitan, termasuk pemilik, perlu dibangunkan dan dikekalkan. Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh Pegawai atau Pegawai Penerima Aset masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Memastikan semua aset ICT dikenalpasti dan maklumat aset direkod serta sentiasa dikemaskini dalam borang daftar harta modal dan inventori; (b) Memastikan semua aset ICT mempunyai Pemilik dan dikendalikan oleh Pengguna yang dibenarkan sahaja; (c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di LHDNM;	Pegawai Aset Pegawai Penerima Aset

ID	KETERANGAN	PERANAN
	(d) Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, didokumenkan dan dilaksanakan; dan (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	
1.10 Penggunaan Maklumat yang Boleh Diterima dan Aset Lain yang Berkaitan		
1.10.1	**Penggunaan Maklumat yang Boleh Diterima dan Aset Lain yang Berkaitan** Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut termasuk Arahan Teknologi Maklumat : (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 piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan,	Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; (h) Sekatan capaian yang menyokong keperluan perlindungan untuk setiap peringkat pengelasan; dan (i) Penyelenggaraan rekod pengguna yang dibenarkan bagi maklumat dan aset lain yang berkaitan.	
1.11 Pemulangan Aset		
1.11.1	**Pemulangan Aset** Pegawai dan kakitangan serta pihak berkaitan perlu mengembalikan semua aset organisasi dalam pemilikan mereka apabila berlaku perubahan atau penamatan pekerjaan, kontrak atau perjanjian mereka. Perkara-perkara yang perlu dipatuhi termasuk: (a) Memastikan semua aset ICT dikembalikan kepada LHDNM mengikut peraturan dan/atau terma dan syarat perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan memproses maklumat mengikut	Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	peraturan dan/atau terma dan syarat perkhidmatan yang ditetapkan.	
1.12 Pengelasan Maklumat		
1.12.1	**Pengelasan Maklumat** Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Dasar Keselamatan Perlindungan Lembaga Hasil Dalam Negeri Malaysia. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Dasar Keselamatan Perlindungan Lembaga Hasil Dalam Negeri Malaysia seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	Warga Hasil Pihak Ketiga
1.13 Pelabelan Maklumat		
1.13.1	**Pelabelan Maklumat** Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Dasar Keselamatan Perlindungan Lembaga Hasil Dalam Negeri Malaysia.	Warga Hasil

ID	KETERANGAN	PERANAN
1.14 Pemindahan Data dan Maklumat		
1.14.1	**Polisi dan Prosedur Pemindahan Data dan Maklumat** LHDNM perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara LHDNM dengan pihak luar serta mematuhi Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional. Perkara yang perlu dipertimbangkan ialah : (a) Penghantaran dan penerimaan maklumat LHDNM hendaklah dalam keadaan terkawal; (b) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat LHDNM; (c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan (d) LHDNM hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan mencegah ketirisan data.	Warga Hasil
1.14.2	**Pengurusan Pesanan Elektronik (Electronic Messaging Management)** Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan	Warga Hasil

ID	KETERANGAN	PERANAN
	peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti **Lampiran A** : (a) Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003; (b) Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 - Pematuhan Tatacara Penggunaan E-mel dan Internet; dan Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa.	
1.14.3	**Perjanjian Kerahsiaan atau Ketakdedahan (Confidentiality Or Non-Disclosure Agreement)** Syarat-syarat perjanjian kerahsiaan atau *Non-Disclosure Agreements* (NDA) perlu mengambil kira keperluan organisasi dan hendaklah disemak, dikemaskini dan didokumentasikan. Pembekal / agensi luar hendaklah bersetuju dengan terma dan syarat perjanjian dan berakujanji mematuhi semua keperluan keselamatan maklumat.	ICTSO Pengarah Bahagian Pentadbir Sistem ICT Pengguna Pembekal

ID	KETERANGAN	PERANAN
1.14.4	**Pencegahan Kebocoran Data (Data Leakage Prevention)** LHDNM bertanggungjawab untuk memastikan bahawa maklumat sensitif atau sulit tidak didedahkan atau dibocorkan dan hanya boleh diakses oleh individu yang dibenarkan sahaja untuk mencegah penyalahgunaan maklumat. Pencegahan ini penting untuk melindungi privasi individu dan keselamatan organisasi.	CDO ICTSO Pengarah Bahagian Pentadbir Sistem ICT Pengguna Pembekal
1.15 Kawalan Akses & Pengurusan Identiti		
1.15.1	**Polisi Kawalan Capaian** Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumentasikan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;	Pengurus ICT Pentadbir Keselamatan ICT Pentadbir Rangkaian ICT Pentadbir Sistem ICT Pemilik Sistem ICT

ID	KETERANGAN	PERANAN
	(b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	
1.15.2	**Akaun Pengguna** Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenalpasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi : (a) Akaun pengguna yang diperuntukkan oleh LHDNM sahaja boleh digunakan; (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Akaun pengguna yang diwujudkan hendaklah mengikut peranan yang ditetapkan. Sebarang perubahan tahap capaian perlu mendapat kelulusan daripada Pemilik Sistem ICT dan Pentadbir Sistem Operasi; (d) Pemilikan akaun pengguna bukanlah hak mutlak pengguna dan ia tertakluk kepada peraturan LHDNM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Perkongsian akaun pengguna adalah dilarang sama sekali; dan	CDO Pengurus ICT Pentadbir Sistem ICT Pentadbir Sistem Operasi Warga Hasil

ID	KETERANGAN	PERANAN
	(f) CDO, Pengurus ICT, Pemilik Sistem ICT atau Pentadbir Sistem Operasi boleh membeku atau menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna yang bercuti atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain (kecuali MOF); iv. Bersara; atau v. Ditamatkan atau digantung perkhidmatan. (g) Capaian kepada emel dan Aplikasi Umum di Hasil Identity (HI) seperti Sistem Pengurusan Insan (SPI), e-Kewangan dan Hasilpedia diberikan secara automatik kepada pegawai seperti berikut: i. Pengguna yang bercuti atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan; dan ii. Bertukar ke agensi lain (MOF sahaja) (h) Capaian kepada sistem di bawah Aplikasi Korporat di Hasil Identity (HI) seperti Hasil Integrated Tax System (HITS), Case Management System (CMS), Revenue Management System (ReMS), diberikan berdasarkan merit / justifikasi keperluan tugasan pegawai. (i) Semakan semula semua sistem dibawah Aplikasi Umum di HI. Kenalpasti capaian kepada sesuatu sistem samada boleh dicapai	

ID	KETERANGAN	PERANAN
	oleh semua pegawai atau berdasarkan profil dan bidang tugas pegawai.	
1.15.3	**Hak Capaian** Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	CDO Pengurus ICT Pemilik Sistem ICT Pentadbir Sistem ICT
1.15.4	**Kajian Semula Hak Capaian Pengguna** Pentadbir aset hendaklah menyemak hak capaian pengguna secara berkala sekurang-kurangnya sekali dalam tempoh setahun. Pentadbir Sistem perlu mewujudkan rekod pendaftaran dan penamatan pengguna sistem masing-masing sebagai rujukan semakan ke atas hak capaian pengguna secara berkala. Semakan ke atas hak capaian fizikal dan logik harus mempertimbangkan perkara berikut: (a) Hak capaian pengguna selepas sebarang perubahan dalam organisasi (contohnya pertukaran pekerjaan, kenaikan pangkat, penurunan pangkat) atau penamatan perkhidmatan/pekerjaan; dan (b) Kebenaran untuk hak capaian istimewa.	Pentadbir Aset Pentadbir Sistem Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM

ID	KETERANGAN	PERANAN
1.15.5	**Pengurusan Kata Laluan** Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai aset ICT LHDNM mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh LHDNM seperti berikut: (a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan sekurang-kurangnya tiga (3) daripada empat (4) item berikut: i. Huruf besar; ii. Huruf kecil; iii. Nombor; atau iv. Simbol. (d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;	CDO Pengurus ICT Pentadbir Keselamatan ICT Pentadbir Sistem ICT Pemilik Sistem ICT Warga Hasil

ID	KETERANGAN	PERANAN
	(g) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas kata laluan ditetapkan semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; (j) Jenis Kata Laluan dibahagikan kepada dua kategori iaitu : i. Pengguna Biasa ii. *Service Account* Untuk akaun pengguna biasa, kata laluan hendaklah ditukar selepas sembilan puluh (90) hari. Bagi akaun kategori *Service Account*, proses penukaran kata laluan hendaklah dilakukan sekali dalam setahun. (k) Mengelakkan penggunaan semula empat (4) kata laluan terakhir yang telah digunakan sebelum ini.	
1.16 Maklumat Pengesahan Identiti		
1.16.1	**Pengurusan Maklumat Pengesahan Rahsia Pengguna (Management of Secret Authentication Information of Users)**	CDO Pentadbir Sistem ICT Warga Hasil

ID	KETERANGAN	PERANAN
	Peranan dan tanggungjawab pengguna adalah seperti yang berikut : (a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber LHDNM; (b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; (c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat LHDNM; (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, penyampaian, pertukaran dan pemusnahan; dan;	

ID	KETERANGAN	PERANAN
	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.	
1.16.2	**Penggunaan Maklumat Pengesahan Rahsia (Use of Secret Authentication Information)** Pengguna perlu mengikut amalan keselamatan yang baik dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.	Pentadbir Sistem ICT Warga Hasil
1.17 Hak Akses Pengurusan Capaian Pengguna		
1.17.1	**Pendaftaran dan Pembatalan Pengguna (User Registration and Deregistration)** Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi : (a) Akaun yang diperuntukkan oleh LHDNM sahaja boleh digunakan; (b) Akaun pengguna mestilah unik;	Pentadbir Sistem ICT Warga Hasil

ID	KETERANGAN	PERANAN
	(c) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada LHDNM terlebih dahulu; (d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (e) Pemilikan akaun bukanlah hak mutlak pengguna dan boleh ditarik balik jika penggunaannya melanggar peraturan LHDNM; dan (f) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan LHDNM dan didokumentasikan.	
1.17.2	**Peruntukan Akses Pengguna (User Access Provisioning)** Proses formal peruntukan akses pengguna perlu dilaksanakan dalam pemberian atau pembatalan hak akses kepada semua jenis pengguna termasuk sistem dan perkhidmatan. Proses peruntukan untuk memberi atau membatalkan hak akses yang diberikan kepada ID Pengguna perlu merangkumi : (a) Mendapatkan kebenaran daripada pemilik sistem atau perkhidmatan ICT; (b) Menentusahkan tahap akses yang diberikan adalah wajar dan selaras dengan keperluan tugas;	Pengarah Bahagian Pentadbir Sistem ICT Warga Hasil

ID	KETERANGAN	PERANAN
	(c) Memastikan hak akses tidak diaktifkan sebelum prosedur kebenaran dilengkapkan; (d) Mengekalkan rekod berpusat untuk hak akses yang diberikan kepada ID Pengguna; (e) Menyesuaikan hak akses pengguna yang menukar peranan atau pekerjaan dan segera menyekat atau menghapuskan hak akses pengguna yang telah meninggalkan organisasi; dan (f) Mengkaji semula secara berkala hak akses tersebut.	
1.17.3	**Pengurusan Hak Akses Istimewa (Management of Privileged Access Rights)** 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 prosedur pendaftaran, perubahan dan penamatan pengguna.	Pentadbir Sistem ICT
1.18 Keselamatan Maklumat dalam Hubungan Dengan Pembekal		
1.18.1	**Polisi Keselamatan Siber untuk Hubungan Dengan Pembekal** Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset LHDNM.	Pengarah Bahagian Pemilik Projek Pembekal

ID	KETERANGAN	PERANAN
	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; (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 LHDNM kepada pembekal; (h) Menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber LHDNM (Lampiran 1B)**; dan (i) Pembekal perlu mematuhi Dasar Keselamatan Perlindungan Lembaga Hasil Dalam Negeri Malaysia yang berkuatkuasa.	

ID	KETERANGAN	PERANAN
1.19 Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal		
1.19.1	**Menangani Keselamatan Dalam Perjanjian Dengan Pembekal** Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua pegawai dan kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak LHDNM selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, LHDNM mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) LHDNM 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;	Syarikat Pembekal

ID	KETERANGAN	PERANAN
	(c) Semua wakil syarikat pembekal hendaklah melepasi tapisan 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 maklumat yang relevan bagi mengakses, memproses,	

ID	KETERANGAN	PERANAN
	menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan LHDNM; dan (h) Syarikat pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh LHDNM. (i) Akses kepada aset ICT LHDNM perlu berlandaskan kepada perjanjian kontrak; (j) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan Pihak Ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai : i. Polisi Keselamatan Siber LHDNM; ii. Perakuan Akta Rahsia Rasmi 1972; iii. Hak Harta Intelek; dan iv. Undang-undang dan Peraturan semasa yang dikuatkuasa. (k) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber LHDNM sebagaimana **Lampiran 1B**	
1.20 Menguruskan Keselamatan Maklumat Dalam Rantaian Bekalan ICT		
1.20.1	**Rantaian Bekalan Teknologi Maklumat dan Komunikasi**	Pengarah Bahagian Pembekal

ID	KETERANGAN	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 subkontraktor atau 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.	Pemilik Projek
1.21 Pemantauan, Semakan Dan Pengurusan Perubahan Bagi Perkhidmatan Pembekal		
1.21.1	**Memantau dan Mengkaji Semula Perkhidmatan Pembekal (Monitoring and Review Supplier Services)** LHDNM hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:	Pengarah Bahagian Pembekal Pemilik Projek

ID	KETERANGAN	PERANAN
	i. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; ii. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	
1.21.2	**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 perkhidmatan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut : i. Perubahan dalam perjanjian dengan pembekal; ii. Perubahan yang dilakukan oleh LHDNM bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan iii. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru,	Pengarah Bahagian Pembekal Pemilik Projek

ID	KETERANGAN	PERANAN
	perubahan lokasi, pertukaran pembekal dan subkontraktor.	
1.22	**Keselamatan Maklumat Dalam Penggunaan Perkhidmatan Pengkomputeran Awan**	
1.22.1	**Keselamatan Maklumat Dalam Penggunaan Perkhidmatan Pengkomputeran Awan** Pengurusan perkhidmatan awan ini melibatkan pelbagai aspek teknikal dan pentadbiran untuk memastikan perkhidmatan awan digunakan secara berkesan, selamat dan sesuai dengan keperluan organisasi. Perkara berikut perlu dipatuhi oleh semua pihak yang terlibat: Memastikan kepatuhan terhadap keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak yang berkaitan antaranya : PK 2.6 : Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam; Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam; Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan dalam Perkhidmatan Awam. Pengurusan perkhidmatan yang disediakan oleh pembekal yang dilantik oleh pihak Kerajaan; Menentukan / mentakrifkan dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan;	CDO ICTSO

ID	KETERANGAN	PERANAN
	Memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan; dan Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	
1.23 Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat		
1.23.1	**Tanggungjawab dan Prosedur** Proses, prosedur dan sistem pemantauan yang lengkap perlu diadakan bagi mengumpul maklumat berkaitan insiden keselamatan ICT. Maklumat tersebut perlu disimpan dan dianalisis bagi tujuan : (a) Perancangan; (b) Tindakan pengukuhan dan pembelajaran; (c) Mengawal kekerapan kerosakan dan kos insiden akan datang; dan (a) Kajian impak kepada LHDNM Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti bagi semua bahan bukti;	ICTSO Pentadbir Keselamatan ICT

ID	KETERANGAN	PERANAN
	(b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	
1.24 Penilaian dan Keputusan Mengenai Keselamatan Maklumat		
1.24.1	**Penilaian dan Keputusan Mengenai Insiden Keselamatan Maklumat** Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Polisi Keselamatan Siber sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan NACSA dengan kadar segera sekiranya : (a) Aset ICT didapati hilang, disyaki hilang, digunakan tanpa kebenaran dan/atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;	ICTSO Pentadbir Keselamatan ICT Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	(c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insideninsiden yang tidak dijangka. Rujuk Lampiran 2, Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT LHDNM. Prosedur pelaporan insiden keselamatan ICT berdasarkan Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022.	
1.25 Tindak Balas Terhadap Insiden Keselamatan Maklumat		
1.25.1	**Tindak Balas Terhadap Insiden Keselamatan** Insiden keselamatan maklumat hendaklah ditangani mengikut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan **Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT (CSIRT) LHDNM**. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut :	ICTSO CSIRT LHDNM

ID	KETERANGAN	PERANAN
	(a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; (b) Menjalankan kajian forensik sekiranya perlu; (c) Menghubungi pihak yang berkenaan dengan secepat mungkin; (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.	
1.26 Pengajaran Daripada Insiden Keselamatan Maklumat		
1.26.1	**Pembelajaran Daripada Insiden Keselamatan Maklumat** Pengajaran 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	ICTSO CSIRT LHDNM

ID	KETERANGAN	PERANAN
	keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	
1.27 Pengumpulan Bahan Bukti		
1.27.1	**Pengumpulan Bahan Bukti** LHDNM hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	ICTSO CSIRT LHDNM
1.28 Keselamatan maklumat semasa gangguan		
1.28.1	**Keselamatan maklumat semasa gangguan** Keselamatan maklumat semasa gangguan merujuk kepada langkah-langkah dan prosedur yang diambil untuk melindungi dan mengekalkan keselamatan maklumat, data, dan sistem ICT semasa terjadi gangguan, bencana atau insiden yang boleh mengancam integriti dan ketersediaan maklumat. Gangguan ini termasuk pelbagai situasi seperti serangan siber, bencana alam, kebakaran, banjir, kecurian, atau insiden teknikal yang tidak diingini. Aspek penting berkaitan dengan keselamatan maklumat semasa gangguan yang perlu diberi perhatian ialah seperti yang berikut: (a) LHDNM hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan	Koordinator PKP Pasukan Pemulihan Bencana ICT CSIRT

ID	KETERANGAN	PERANAN
	maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana; dan (b) Dalam merancang kesinambungan keselamatan maklumat, LHDNM perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi LHDNM.	
1.29 Kesediaan ICT untuk Kesinambungan Perkhidmatan		
1.29.1	**Pelan Kesinambungan Perkhidmatan** Proses Pengurusan Kesinambungan Perkhidmatan (PKP), perlu dilaksanakan untuk meminimakan impak ke atas organisasi dan pemulihan dari bencana sehingga ke tahap toleransi LHDNM sekiranya terdapat gangguan kepada fungsi melalui kombinasi kawalan pencegahan dan pemulihan. Antara elemen pengurusan kesinambungan operasi yang perlu diambil kira dalam pengurusan proses ialah : (a) Memahami risiko yang dihadapi organisasi termasuk mengenalpasti dan memberi keutamaan kepada operasi perkhidmatan yang kritikal; (b) Menentukan proses yang kritikal, pegawai dan kakitangan utama dan sandaran bagi tujuan pemulihan rangkaian, pangkalan data, Pusat Data, sistem aplikasi, sistem komunikasi dan bencana;	Koordinator PKP Pengurus ICT

ID	KETERANGAN	PERANAN
	(c) Menentukan peranan dan tanggungjawab semua pihak yang terlibat dalam program PKP. Rujuk dokumen Pengurusan Kesinambungan Perkhidmatan agensi Sektor Awam Rujukan MAMPU. BPICT.700-4/2/11(3), Lampiran C : Peranan dan Tanggungjawab; (d) Menjadikan pelaksanaan PKP sebagai agenda tetap dalam mesyuarat pengurusan LHDNM dan diterapkan sebagai budaya kerja agensi; (e) Mendapatkan sokongan padu dan komitmen daripada Pengurusan Atasan LHDNM; dan (f) Mendapatkan kelulusan dan pengesahan daripada Pengurusan Atasan LHDNM bagi semua dokumen PKP. Pelan PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: i. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; ii. Senarai pegawai dan kakitangan LHDNM dan pembekal berserta nombor yang boleh dihubungi (telefon dan e-mel). Senarai kedua juga hendaklah disediakan bagi menggantikan pegawai dan kakitangan yang tidak dapat hadir untuk menangani insiden; iii. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;	

ID	KETERANGAN	PERANAN
	iv. Alternatif sumber pemprosesan dan lokasi untuk mengganti - gantikan sumber yang telah lumpuh; dan v. Penjanjian dengan pembekal perkhidmatan untuk mendapat keutamaan penyambungan semula perkhidmatan mengikut kesesuaian. Salinan pelan PKP perlu disimpan di tempat yang berasingan bagi mengelak kerosakan akibat bencana di lokasi utama. Pelan PKP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi niaga untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan kakitangan yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. LHDNM hendaklah memastikan salinan pelan PKP sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	
1.29.2	**Penilaian terhadap Kesinambungan Perkhidmatan dan Risiko** Peristiwa yang boleh mencetuskan gangguan kepada proses perkhidmatan perlu dikenal pasti. Koordinator PKP perlu mengumpul maklumat untuk menentukan	Koordinator PKP Pengurus ICT

ID	KETERANGAN	PERANAN
	strategi yang sesuai. Hasil pengumpulan maklumat perlu didokumenkan dalam laporan penilaian risiko. Melalui laporan penilaian risiko, kelemahan bidang–bidang yang berkaitan dapat dikenal pasti dan seterusnya menentukan tindakan pengawalan atau pencegahan. Antara aktiviti yang terlibat ialah mengenalpasti semua jenis ancaman dalaman dan luaran terhadap perkhidmatan yang diberikan:- (a) Tentukan risiko berdasarkan ancaman; (b) Tentukan tindakan kawalan dan tahap keberkesanan mekanisme kawalan yang sedia ada; dan (c) Sediakan laporan penilaian risiko dan penemuan risiko serta cadangan penambahbaikan untuk diserahkan kepada pengurusan atasan LHDNM. Analisa impak perkhidmatan adalah bertujuan untuk mengenal pasti fungsi–fungsi kritikal perkhidmatan, tempoh pemulihan, sumber–sumber operasi dan kewangan minimum yang diperlukan. Antara aktiviti yang terlibat adalah seperti berikut : i. Mendapatkan peruntukan tahunan LHDNM bagi melaksanakan PKP LHDNM; ii. Mewujudkan Jawantankuasa Kerja Kecil bagi setiap pemilik perkhidmatan;	

ID	KETERANGAN	PERANAN
	iii. Menyenaraikan fungsi atau perkhidmatan agensi LHDNM mengikut keutamaan; iv. Menentukan objektif masa pemulihan mengikut keutamaan perkhidmatan; v. Kenalpasti data lampau yang mungkin hilang dalam selang masa (interval time) yang boleh diterima berdasarkan objektif masa pemulihan; dan vi. Mendokumenkan dan melaporkan semua hasil penemuan kepada Pengurusan Atasan LHDNM.	
1.29.3	**Membangunkan dan melaksanakan Pelan PKP** Berdasarkan hasil penilaian risiko dan analisa impak yang dilaksanakan, strategi yang sesuai dirangka bagi melaksanakan Pengurusan Kesinambungan Perkhidmatan. Strategi yang sesuai adalah untuk: (a) Mengelakkan berlakunya gangguan atau bencana ke atas sistem penyampaian perkhidmatan LHDNM; (b) Segera bertindak apabila berlaku gangguan atau bencana; dan (c) Melaksanakan tindakan segera pemulihan supaya sistem penyampaian perkhidmatan agensi kembali secara normal sepenuhnya. Pelan PKP dibangunkan apabila strategi pelaksanaan dipersetujui :	Koordinator PKP Pengurus ICT

ID	KETERANGAN	PERANAN
	i. Pelan PKP mengandungi prosedur–prosedur dan tindakan–tindakan yang perlu dilaksanakan bagi menangani keadaan kecemasan atau berlaku bencana termasuk pelan komunikasi; dan ii. Pengwujudan Pusat Pemulihan Perkhidmatan LHDNM. Pembangunan dan penerimaan PKP hendaklah dilaksanakan secara berterusan bagi memastikan keberkesanannya. Di antara program yang dicadangkan dalam pelaksanaan PKP ialah : i. Program kesedaran dan latihan perlu diadakan untuk memberi pendedahan kepada PKP dan pentingnya pelaksanaan kepada agensi. Latihan adalah untuk melengkapkan pegawai yang terlibat dengan kemahiran yang diperlukan supaya tanggungjawab dan peranan dapat dilaksanakan dengan berkesan; ii. Program Pengujian / Simulasi dijalankan sekurang- kurangnya sekali setahun untuk membiasakan pasukan PKP LHDNM dengan peranan dan tanggungjawab; iii. Program Penyenggaraan PKP memerlukan semua aktiviti dan komponen PKP diselenggara secara berkala bagi menjamin ketersediaannya. Pelan PKP harus dikaji semula dari semasa ke semasa dan mengemaskini buku panduan PKP; dan	

ID	KETERANGAN	PERANAN
	iv. Program Audit PKP bertujuan untuk memastikan program PKP bersesuaian dan berkesan.	
1.30 Keperluan Perundangan dan Kontrak		
1.30.1	**Pematuhan terhadap Keperluan Perundangan dan Kontrak** Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga hasil, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di LHDNM dan pembekal seperti di **Lampiran A.**	Warga Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM
1.31 Hak Harta Intelek		
1.31.1	**Hak Harta Intelek** Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya LHDNM menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah difetapkan atau dibenarkan.	Warga Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM

ID	KETERANGAN	PERANAN
1.32 Perlindungan Rekod		
1.32.1	**Perlindungan Rekod** 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 Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM
1.33 Privasi dan Perlindungan Maklumat Peribadi		
1.33.1	**Privasi dan Perlindungan Maklumat Peribadi** Maklumat peribadi merujuk kepada sebarang data yang boleh digunakan untuk mengenal pasti individu seperti nombor kad pengenalan, nombor rujukan percukaian dan lain-lain. Pelaksanaan perlindungan maklumat peribadi di LHDNM adalah selaras dengan peruntukan yang dinyatakan dalam Akta Perlindungan Data Peribadi yang terkini.	Warga Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM
1.34 Kajian Semula Keselamatan Maklumat Secara Berkecuali		
1.34.1	**Kajian Semula Keselamatan Maklumat Secara Berkecuali** Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pengarah Bahagian Pemilik Perkhidmatan

ID	KETERANGAN	PERANAN
1.35 Pematuhan Dasar, Peraturan Dan Piawaian Untuk Keselamatan Maklumat		
1.35.1	**Pematuhan Polisi Dan Piawaian Keselamatan** LHDNM hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.	Pengarah Bahagian Pemilik Perkhidmatan
1.36 Prosedur Operasi Yang Didokumenkan		
1.36.1	**Dokumentasi Prosedur Operasi Standard** Prosedur operasi untuk kemudahan pemprosesan maklumat hendaklah didokumenkan dan disediakan kepada pegawai dan kakitangan yang memerlukannya. Perkara-perkara yang perlu dipatuhi termasuk: (a) Semua prosedur operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Timbalan Ketua Pengarah (Operasi Percukaian)

BIDANG 2 : KAWALAN MODAL INSAN

ID	KETERANGAN	PERANAN
2.1 Tapisan Keselamatan		
2.1.1	**Tapisan Keselamatan (Security Screening)** Pemeriksaan pengesahan latar belakang ke atas semua calon untuk menjadi pegawai dan kakitangan hendaklah dijalankan sebelum menyertai organisasi dan secara berterusan dengan mengambil kira undang-undang, peraturan yang berkenaan dan etika dan berkadar dengan keperluan perkhidmatan, klasifikasi maklumat yang akan menjadi diakses dan risiko yang dirasakan. Perkara-perkara yang mesti dipatuhi adalah termasuk: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab Warga Hasil serta Pihak Ketiga yang terlibat bagi menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menguruskan tapisan keselamatan untuk Warga Hasil berasaskan keperluan perundangan dan peraturan selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; (c) Pihak Ketiga perlu mematuhi undang-undang dan peraturan semasa yang dikuatkuasa; (d) Mematuhi syarat perkhidmatan serta peraturan semasa yang dikuatkuasa.	Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
2.2 Terma dan Syarat Perkhidmatan		
2.2.1	**Terma dan Syarat Perkhidmatan** Persetujuan berkontrak dengan Warga Hasil, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM 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 Hasil, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM 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 Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM
2.3 Kesedaran, Pendidikan Dan Latihan Tentang Keselamatan Maklumat		
2.3.1	**Kesedaran, Pendidikan Dan Latihan Tentang Keselamatan Maklumat** Warga Hasil, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan	Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Warga Hasil serta Pihak Ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan; (b) Latihan kesedaran dan yang berkaitan pengurusan keselamatan aset ICT, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk / fungsi / aplikasi / sistem keselamatan perlu diberi secara berterusan (sekiranya perlu) dalam melaksanakan tugas-tugas dan tanggungjawab mereka; dan (c) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul.	
2.4 Proses Tatatertib		
2.4.1	**Proses Tatatertib** Proses formal tindakan disiplin dan / atau undang-undang perlu ditentukan dan disampaikan ke atas Warga Hasil serta Pihak Ketiga yang berkepentingan sekiranya berlaku pelanggaran dan percanggahan peraturan yang telah ditetapkan oleh LHDNM.	Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Memastikan adanya proses tindakan disiplin dan/atau undang-undang sekiranya berlaku pelanggaran terhadap polisi, perundangan dan peraturan yang ditetapkan oleh LHDNM atau Kerajaan; dan; (b) Tindakan tatatertib atau tindakan yang sewajarnya akan dikenakan bagi sebarang pelanggaran kepada polisi ini.	
2.5 Tanggungjawab Selepas Penamatan Atau Perubahan Jawatan		
2.5.1	**Penamatan Atau Pertukaran Peranan Atau Jawatan** Warga Hasil yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut: (a) Memastikan semua aset ICT dikembalikan kepada LHDNM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan LHDNM dan/atau terma perkhidmatan yang ditetapkan. (c) Maklumat rasmi LHDNM dalam peranti tidak dibenarkan dibawa keluar dari LHDNM.	Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	Warga Hasil yang telah bertukar perkhidmatan hendaklah: (a) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada LHDNM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	
2.6 Perjanjian Kerahsiaan atau Ketakdedahan		
2.6.1	**Perjanjian Kerahsiaan atau Ketakdedahan** Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak, dikemaskini dan didokumentasikan. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	ICTSO Pengarah Bahagian Pentadbir Sistem ICT Pengguna Pembekal
2.7 Bekerja Secara Jarak Jauh		
2.7.1	**Bekerja Secara Jarak Jauh** Langkah-langkah keselamatan perlu dilaksanakan apabila pegawai dan kakitangan bekerja secara jarak jauh untuk melindungi maklumat dicapai, diproses atau disimpan di luar organisasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	(a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salahguna kemudahan. (b) Kerahsiaan dan keselamatan semua aset ICT LHDNM yang dicapai atau diguna pakai semasa bekerja dari luar pejabat.	
2.8 Pelaporan Insiden Keselamatan Maklumat		
2.8.1	**Pelaporan Insiden Keselamatan Maklumat** Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat berdasarkan pekeliling atau prosedur pengendalian insiden yang sedang berkuat kuasa. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menentukan mekanisme untuk melaporkan sebarang insiden melalui saluran dan dalam tempoh masa yang ditentukan; (b) Memberi kesedaran berkaitan prosedur pengendalian insiden dan hebahan kepada Warga Hasil sekiranya terdapat perubahan; dan (c) Memastikan Warga Hasil yang mengurus insiden mempunyai kompetensi yang diperlukan.	ICTSO Pengarah Bahagian CSIRT

ID	KETERANGAN	PERANAN
	Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT LHDNM berdasarkan prosedur pengendalian insiden yang sedang berkuat kuasa.	

BIDANG 3 : KAWALAN FIZIKAL

ID	KETERANGAN	PERANAN
3.1 Perimeter Keselamatan Fizikal		
3.1.1	**Perimeter Keselamatan Fizikal** Perimeter keselamatan harus ditakrifkan dan digunakan untuk melindungi kawasan yang mengandungi maklumat dan lain-lain aset bersekutu. lni bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan Aset ICT LHDNM. 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 pegawai dan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan fasiliti pejabat; (d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan	CEO CDO ICTSO Bahagian Keselamatan

ID	KETERANGAN	PERANAN
	sebarang bencana alam atau perbuatan manusia; (e) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk pegawai dan 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.	
3.2 Kawalan Kemasukan Fizikal		
3.2.1	**Kawalan Kemasukan Fizikal** Kawasan selamat harus dilindungi oleh kawalan masuk dan akses yang sesuai. Perkara-perkara yang perlu dipatuhi adalah termasuk: (a) Setiap Warga Hasil hendaklah memakai atau mengenakan Kad Pengenalan Jabatan semasa ingin memasuki atau berada dalam kawasan dan bangunan LHDNM; (b) Semua Kad Pengenalan Jabatan hendaklah diserahkan kembali kepada Bahagian Keselamatan LHDNM apabila Pengguna berhenti atau ditamatkan perkhidmatan;	Seksyen Keselamatan ICT Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	(c) Setiap Pelawat hendaklah mendaftar dan mendapatkan Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; (d) Kehilangan Kad Pengenalan Jabatan atau Pas Keselamatan Pelawat hendaklah dilaporkan kepada Bahagian Keselamatan LHDNM.	
3.3 Keselamatan Pejabat, Bilik dan Fasiliti		
3.3.1	**Keselamatan Pejabat, Bilik dan Kemudahan** 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 berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan (c) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi Dasar Keselamatan Perlindungan Lembaga Hasil Dalam Negeri Malaysia.	Warga Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM

ID	KETERANGAN	PERANAN
3.4 Pemantauan Keselamatan Fizikal		
3.4.1	**Pemantauan Keselamatan Fizikal** Kawalan pemantauan keselamatan fizikal perlu dipantau secara berterusan bagi mengelakkan akses tanpa kebenaran daripada pihak yang tidak bertanggungjawab.	Bahagian Keselamatan
3.5 Perlindungan Daripada Ancaman Fizikal dan Persekitaran		
3.5.1	**Perlindungan Daripada Ancaman Fizikal dan Persekitaran** Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. LHDNM perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau, bencana dan wabak penyakit.	Pentadbir Pusat Data BPPF
3.6 Bekerja di Kawasan Selamat		
3.6.1	**Bekerja di Kawasan Selamat** Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi Warga Hasil yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis LHDNM termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti	Pentadbir Pusat Data BPPF

ID	KETERANGAN	PERANAN
	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 Hasil 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; QO (e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; (f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang 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	

ID	KETERANGAN	PERANAN
	(j) Mengehadkan jalan keluar masuk.	
3.7 Polisi Meja Kosong dan Skrin Kosong		
3.7.1	**Polisi Meja Kosong dan Skrin Kosong** Polisi Meja Kosong dan Skrin Kosong bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna, pada paparan skrin komputer, mesin pencetak, mesin faksimili atau mesin pengimbas apabila pengguna tidak berada di tempatnya. Polisi Meja Kosong dan Skrin Kosong ialah satu set garis panduan yang digunakan dalam pengurusan keselamatan maklumat dan keberkesanan dalam organisasi untuk melindungi maklumat sensitif dan menjaga privasi pekerja. Objektif utama polisi ini adalah untuk memastikan data dan maklumat terjamin keselamatannya dan tidak didedahkan kepada pihak yang tidak mempunyai hak capaian ke atas data atau maklumat tersebut. Polisi ini merangkumi aspek-aspek berikut: (a) Menggunakan kemudahan kata laluan penyelamat skrin (screensaver password) atau log keluar (logout) apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;	Warga Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM

ID	KETERANGAN	PERANAN
	(c) Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat. (d) E-mel masuk dan keluar hendaklah dikawal; dan (e) Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	
3.8 Penempatan dan Perlindungan Peralatan ICT		
3.8.1	**Penempatan dan Perlindungan Peralatan ICT** Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut: (a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;	Warga Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM

ID	KETERANGAN	PERANAN
	(d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; (e) 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; (f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna; (g) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; (h) Peralatan-peralatan kritikal perlu disokong oleh Uninterruptable Power Supply (UPS) dan Generator Set (Gen-Set); (i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. (j) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci; (k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai;	

ID	KETERANGAN	PERANAN
	(l) Peralatan ICT yang hendak dibawa ke luar premis LHDNM, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; (m) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; (n) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT; (p) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; (q) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) Konfigurasi Alamat IP juga tidak dibenarkan diubah daripada Alamat IP yang asal; (s) Pengguna dilarang sama sekali mengubah password administrator yang telah ditetapkan oleh pihak ICT; dan	

ID	KETERANGAN	PERANAN
	(t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan LHDNM sahaja.	
3.9 Keselamatan Aset Di Luar Premis		
3.9.1	**Keselamatan Aset Di Luar Premis** Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis LHDNM. Peralatan yang dibawa keluar dari premis LHDNM adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Warga Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM
3.10 Media Storan		
3.10.1	**Pengurusan Media Boleh Alih** Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical*	Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	disk, *flash drive*, CDROM, *thumb drive* dan media storan lain. Media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Mengadakan ujian *restore* kepada salinan atau penduaan (*backup*) pada media storan kedua secara berkala. Perkara-perkara yang perlu dipatuhi adalah termasuk: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan sewajarnya berdasarkan kandungan maklumat yang disimpan; (b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pegawai dan kakitangan atau pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah kecurian,kemusnahan dan capaian yang tidak dibenarkan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di tempat yang selamat; (e) Akses dan pergerakan media storan hendaklah direkodkan; (f) Mengadakan salinan atau penduaan (backup) pada media storan kedua bagi	

ID	KETERANGAN	PERANAN
	tujuan keselamatan dan bagi mengelakkan kehilangan data; (g) Perkakasan *backup* hendaklah diletakkan di tempat yang selamat dan terkawal; (h) Semua media storan data yang hendak dilupuskan mestilah mengikut peraturan semasa yang berkuatkuasa; dan (i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan Pemilik Sumber Maklumat terlebih dahulu.	
3.11 Utiliti Sokongan		
3.11.1	**Utiliti Sokongan** 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 Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM
3.12 Keselamatan Kabel		
3.12.1	**Keselamatan Kabel** 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	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	
3.13 Penyelenggaraan Peralatan		
3.13.1	**Penyelenggaraan Peralatan** Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan	Pegawai Aset Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; (c) Memastikan perkakasan hanya diselenggara oleh pegawai dan kakitangan atau pihak yang dibenarkan sahaja; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan (e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
3.14 Pengalihan Aset		
3.14.1	**Pengalihan Aset** Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Peralatan ICT gunasama yang hendak dibawa keluar dari premis LHDNM untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Pengarah LHDNM atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan	Pengguna Pegawai Aset

ID	KETERANGAN	PERANAN
	pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan (b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	
3.15 Keselamatan Peralatan dan Aset di Luar Premis		
3.15.1	**Keselamatan Peralatan dan Aset di Luar Premis** Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis LHDNM. Peralatan yang dibawa keluar dari premis LHDNM adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Warga Hasil Pembekal Pakar Runding Pihak yang mempunyai urusan dengan perkhidmatan ICT LHDNM

ID	KETERANGAN	PERANAN
3.16 Pelupusan Selamat Atau Penggunaan Semula Peralatan		
3.16.1	**Pelupusan Selamat Atau Penggunaan Semula Peralatan** 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. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh LHDNM dan ditempatkan di LHDNM. Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan LHDNM. Langkah-langkah seperti yang berikut hendaklah diambil: (a) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat; (b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang	Pegawai Aset Pentadbir Sistem ICT Warga Hasil

ID	KETERANGAN	PERANAN
	mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (d) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; (e) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti yang berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM, harddisk, motherboard* dan sebagainya. iii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di LHDNM. iv. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak ditupuskan; dan v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab LHDNM.	

ID	KETERANGAN	PERANAN
	(f) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau thumbdrive sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. (g) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan; (h) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa; (i) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Dasar Keselamatan Perlindungan Lembaga Hasil Dalam Negeri Malaysia dan tatacara Jabatan Arkib Negara; dan (j) Pegawai aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori MyAsset.	

BIDANG 4 : KAWALAN TEKNOLOGI

ID	KETERANGAN	PERANAN
4.1 Polisi Peranti Mudah Alih		
4.1.1	**Polisi Peranti Mudah Alih** Maklumat yang disimpan, diproses oleh atau boleh diakses melalui peranti mudah alih pengguna harus dilindungi. Perkara-perkara yang perlu dipatuhi termasuk: (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 atau komponen peralatan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat sebarang pemasangan perisian tambahan atau menggunakan sistem tanpa mendapat kebenaran CDO; (e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;	Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	(f) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dimatikan suis sebelum meninggalkan pejabat; (g) Penggunaan katalaluan untuk membuat capaian kepada sistem komputer adalah diwajibkan; (h) Pengguna hendaklah melindungi semua peralatan sokongan ICT daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (i) Peralatan-peralatan kritikal perlu disokong *uninterruptable power supply* (UPS); (j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switch, hub, router* dan peralatan-peralatan lain yang berkaitan perlu diletakkan di dalam rak khas dan berkunci yang tidak menghalang laluan. Pemasangan peralatan rangkaian dalam rak khas tersebut perlu ditempatkan di dalam bilik khas yang dikenali sebagai *Telecomunication Closet Room* (TCR); (k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai;	

ID	KETERANGAN	PERANAN
	(l) Peralatan ICT yang hendak dibawa keluar dari premis LHDNM, perlulah mendapat kebenaran Penyelaras ICT atau Pentadbir Sistem ICT mengikut peraturan semasa yang berkuatkuasa dan direkodkan oleh Pegawai Aset yang menguruskan peralatan ICT bagi tujuan pemantauan; (m) Peralatan ICT yang hilang hendaklah dilaporkan kepada Pegawai Aset dan ICTSO dengan segera; (n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; (o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa mendapat kebenaran Penyelaras ICT atau Pentadbir Sistem ICT; (p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Penyelaras ICT atau Pentadbir Sistem ICT untuk dibaikpulih; (q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bertujuan bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal tanpa	

ID	KETERANGAN	PERANAN
	mendapat kebenaran Penyelaras ICT atau Pentadbir Sistem ICT; (s) Pengguna adalah dilarang sama sekali mengubah kata laluan administrator yang telah ditetapkan oleh Pentadbir Sistem ICT; (t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (u) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan ditutup apabila meninggalkan pejabat; (v) Sebarang bentuk penyelewengan atau salahguna peralatan ICT hendaklah dilaporkan kepada Penyelaras ICT atau Pentadbir Sistem ICT untuk disalurkan kepada ICTSO; (w) Memastikan soket dicabut dari *switch socket outlet* sebelum meninggalkan pejabat bagi mengelak kerosakan perkakasan yang boleh mengakibatkan litar pintas seperti petir, kilat dan sebagainya; dan (x) Memastikan perisian antivirus sentiasa aktif, dikemaskini dan imbasan dilaksanakan ke atas media storan bagi semua peralatan ICT yang dibekalkan oleh LHDNM.	

ID	KETERANGAN	PERANAN
4.2 Hak Capaian Istimewa		
4.2.1	**Pengurusan Hak Capaian Istimewa** Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenalpasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun pengguna yang diperuntukkan oleh LHDNM sahaja boleh digunakan; (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Akaun pengguna yang diwujudkan hendaklah mengikut peranan yang ditetapkan. Sebarang perubahan tahap capaian perlu mendapat kelulusan daripada ”Pemilik Sistem ICT” dan Pentadbir Sistem Operasi”. ; (d) Pemilikan akaun pengguna bukanlah hak mutlak pengguna dan ia tertakluk kepada peraturan LHDNM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Perkongsian akaun pengguna adalah dilarang sama sekali; dan (f) CDO, Pengurus ICT, Pemilik Sistem ICT atau Pentadbir Sistem Operasi boleh membeku atau menamatkan akaun pengguna atas sebab-sebab berikut:	CDO Pengurus ICT Pentadbir Sistem ICT Pentadbir Sistem Operasi Warga Hasil

ID	KETERANGAN	PERANAN
	(i) Pengguna yang bercuti atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan; (ii) Bertukar bidang tugas kerja; (iii) Bertukar ke agensi lain (kecuali MOF); (iv) Bersara; atau (v) Ditamatkan atau digantung perkhidmatan. (g) Capaian kepada emel dan Aplikasi Umum di Hasil Identity (HI) seperti Sistem Pengurusan Insan (SPI) dan e-Kewangan diberikan secara automatik kepada pegawai seperti berikut: (i) Pengguna yang bercuti atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan; dan (ii) Bertukar ke agensi lain (MOF sahaja) (h) Capaian kepada sistem di bawah milik LHDNM diberikan berdasarkan merit / justifikasi keperluan tugasan pegawai. (i) Semakan semula semua sistem dibawah Aplikasi Umum di HI. Kenalpasti capaian kepada sesuatu sistem samada boleh	

ID	KETERANGAN	PERANAN
	dicapai oleh semua pegawai atau berdasarkan profil dan bidang tugas pegawai.	
4.3 Sekatan Capaian Maklumat		
4.3.1	**Sekatan Capaian Maklumat** Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pentadbir Sistem ICT Pengguna
4.4 Kawalan Capaian Kepada Kod Sumber		
4.4.1	**Kawalan Capaian Kepada Kod Sumber Program** Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan (b) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik LHDNM. (c) Mengurus capaian kepada kod sumber program dan perpustakaan sumber program (program source libraries) mengikut prosedur yang ditetapkan; dan (d) Memberi capaian baca dan tulis kepada kod sumber berdasarkan keperluan dan berupaya mengawal risiko mengubah atau	Pengarah Projek Pengurus Projek Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	menyalah guna kod sumber berdasarkan prosedur yang ditetapkan.	
4.5 Pengesahan Identiti Yang Selamat		
4.5.1	**Pengesahan Identiti Yang Selamat** Kawalan terhadap capaian aplikasi sistem 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 berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan LHDNM; (b) Pendedahan maklumat ketika log masuk mestilah berdasarkan kepada prinsip ‘Atas dasar perlu mengetahui’; (c) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; (d) Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem; (e) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna;	Pentadbir Rangkaian Pentadbir Keselamatan ICT

ID	KETERANGAN	PERANAN
	(f) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; dan (g) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
4.6 Pengurusan Kapasiti		
4.6.1	**Pengurusan Kapasiti** 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 yang berikut: (a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan (b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	CDO ICTSO Pengurus ICT

ID	KETERANGAN	PERANAN
4.7 Perlindungan Daripada Perisian Hasad		
4.7.1	**Perlindungan Daripada Perisian Hasad** 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 dipatuhi termasuk: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) 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) Mengimbas semua perisian atau sistem yang terdapat pada mana-mana media storan dengan sistem antivirus sebelum menggunakannya; (d) Mengemaskini antivirus dengan *pattern* antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan	ICTSO Pentadbir Keselamatan ICT Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; (g) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (h) Mengemaskini *patches* sistem pengoperasian pada peralatan ICT; (i) 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; dan (j) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.	
4.8 Pengurusan Kerentanan Teknikal		
4.8.1	**Pengurusan Kerentanan Teknikal** 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 dilaksanakan ke atas	ICTSO Pentadbir Keselamatan ICT Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	sistem aplikasi dan operasi yang digunakan. Kerentanan sistem operasi dan aplikasi yang digunakan perlu dikawal dengan berkesan. 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.	
4.9 Pengurusan Konfigurasi		
4.9.1	**Pengurusan Konfigurasi** Untuk memastikan perkakasan, perisian, servis dan rangkaian dikawal dengan selamat dan konfigurasi tidak diubah sewenang-wenangnya oleh pihak yang tidak mempunyai hak capaian akses. Setiap konfigurasi perkakasan, perisian dan sistem baharu mestilah dilaksanakan secara teratur dan direkodkan. Dokumentasi dan manual pentadbir hendaklah disimpan secara dalam talian atau fizikal. Sekiranya disimpan secara fizikal, dokumen tersebut mestilah disimpan di ruangan yang selamat.	Pentadbir Sistem ICT Pengurus ICT

ID	KETERANGAN	PERANAN
4.10 Penghapusan Maklumat		
4.10.1	**Penghapusan Maklumat** LHDNM perlu melaksanakan pengurusan pelupusan maklumat yang tidak perlu atau sudah tidak digunakan daripada sistem, peralatan dan perkakasan. Setiap data yang telah dikenalpasti untuk dihapuskan hendaklah menggunakan kaedah hapus kekal (*secure permanently erase*).	Pentadbir Sistem ICT
4.11 Penyembunyian Data		
4.11.1	**Penyembunyian Data** Untuk menghadkan keterdedahan perkongsian visual data-data peribadi dalam pelbagai medium yang boleh mengundang penyalahgunaan data individu. Data yang perlu dilindungi adalah data sensitif seperti *Personal Identifiable Information* (PII) dan data ini tidak boleh dipaparkan dalam paparan pengguna sistem dan sekiranya dikeluarkan daripada sistem, data tersebut perlu digantikan dengan nilai yang tidak dapat dikenalpasti atau dihubungkan kembali ke data asal. Walaubagaimanapun, akaun pentadbir sistem dibenarkan untuk mengakses data sensitif kerana pentadbir sistem bertanggungjawab menguruskan akaun pengguna sistem.	Pentadbir Sistem Aplikasi Pihak Ketiga

ID	KETERANGAN	PERANAN
4.12 Pencegahan Ketirisan Data		
4.12.1	**Pencegahan Ketirisan Data** LHDNM bertanggungjawab untuk memastikan bahawa maklumat sensitif atau sulit tidak didedahkan atau dibocorkan dan hanya boleh diakses oleh individu yang dibenarkan sahaja untuk mencegah penyalahgunaan maklumat. Pencegahan ini penting untuk melindungi privasi individu dan keselamatan organisasi.	CDO ICTSO Pengarah Bahagian Pentadbir Sistem ICT Pengguna Pembekal
4.13 Sandaran Maklumat		
4.13.1	**Sandaran Maklumat** Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah termasuk: (a) Membuat sandaran ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan sandaran adalah bergantung kepada tahap kritikal maklumat; (c) Menguji sistem sandaran dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh	ICTSO Pengurus ICT Pentadbir Keselamatan ICT Pentadbir Sistem ICT Penyelaras ICT Warga Hasil Pihak Ketiga

ID	KETERANGAN	PERANAN
	dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) Menyimpan sekurang-kurangnya tiga (3) generasi sandaran; dan (e) Merekod dan menyimpan salinan sandaran di lokasi yang berlainan dan selamat. Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan, tahunan atau dari semasa ke semasa.	
4.14 Lewahan Kemudahan Pemprosesan Maklumat		
4.14.1	**Lewahan Kemudahan Pemprosesan Maklumat** Kemudahan pemprosesan maklumat LHDNM perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (failover test) keberkesanannya dari semasa ke semasa.	Pentadbir Pusat Data Pemilik Perkhidmatan Pentadbir Sistem ICT
4.15 Pengelogan Maklumat		
4.15.1	**Menyediakan Log** 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.	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	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 fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: (a) Fail log sistem pengoperasian; (b) Fail log servis (contoh: web, e-mel); (c) Fail log aplikasi (audit trail); dan (d) Fail log rangkaian (contoh: switch, firewall, IPS). Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian makiumat dan	

ID	KETERANGAN	PERANAN
	pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada pasukan CSIRT LHDNM.	
4.15.2	**Perlindungan Maklumat Log** Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin merangkumi perkara berikut : (a) Pengguna, termasuk mereka yang mempunyai hak capaian istimewa, tidak diberi kebenaran untuk memadam atau menyahaktifkan log aktiviti mereka sendiri; dan (b) Kemudahan pengelogan beroperasi dengan baik.	Pentadbir Sistem ICT
4.16 Aktiviti Pemantauan		
4.16.1	**Aktiviti Pemantauan** Pentadbir Sistem perlu memantau untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat. Aktiviti pemantauan perlu merangkumi perkara seperti yang berikut: (a) Trafik keluar (outbound) dan masuk (inbound) bagi rangkaian, sistem dan aplikasi; (b) Capaian kepada sistem, pelayan, peralatan rangkaian, sistem pemantauan, aplikasi kritikal; (c) Log daripada peralatan keselamatan (contohnya antivirus, IDS, sistem pencegahan	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	pencerobohan (IPS), penapis web, firewall, pencegahan kebocoran data); (d) Log peristiwa yang berkaitan dengan sistem dan aktiviti rangkaian; (e) Memastikan supaya kod sumber yang dilaksanakan telah diberi kebenaran untuk dilaksanakan dan tidak diubah tanpa kebenaran; dan (f) Penggunaan dan prestasi sumber.	
4.17 Penyegerakan Jam		
4.17.1	**Penyegerakan Jam** Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam LHDNM atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM).	Pentadbir Pusat Data
4.18 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa		
4.18.1	**Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa** Penggunaan program utiliti yang boleh mengatasi (overriding) kawalan sistem dan aplikasi hendaklah dikawal dan dihadkan kepada pegawai yang	Pengarah Bahagian Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	dibenarkan sahaja Perkara yang perlu dipatuhi ialah seperti yang berikut : (a) Had penggunaan program utiliti kepada bilangan praktikal minimum pengguna yang dipercayai dan dibenarkan; (b) Penggunaan prosedur pengenalan, pengesahan dan kebenaran untuk program utiliti, termasuk pengenalan unik pengguna program utiliti; (c) Mentakrif dan mendokumentasikan tahap kebenaran untuk program utiliti; (d) Kebenaran untuk menggunakan program utiliti secara *ad hoc*; (e) Melaksanakan pengasingan tugas dengan menghadkan capaian pengguna yang mempunyai capaian kepada program utiliti; (f) Mengalih keluar atau melumpuhkan semua program utiliti yang tidak diperlukan; (g) Menghadkan ketersediaan program utiliti; dan (h) Pengelogan semua penggunaan program utiliti.	
4.19 Pemasangan Perisian Pada Sistem Operasi		
4.19.1	**Pemasangan Perisian Pada Sistem Operasi** 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:	Pengarah Bahagian Pentadbir Sistem ICT

ID	KETERANGAN	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; (c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur; (d) Pengemaskinian perisian operasi hanya boleh dilaksanakan oleh pentadbir terlatih atas kebenaran pengurusan; (e) Memastikan bahawa hanya kod boleh laksana (executable code) yang telah diluluskan dan tiada kod pembangunan atau pengkompil (compilers) dipasang pada sistem operasi; (f) Mengemas kini semua perpustakaan sumber (source libraries) program yang sepadan; (g) Menggunakan sistem kawalan konfigurasi untuk mengekalkan kawalan semua perisian operasi serta dokumentasi sistem; (h) Mengarkibkan versi lama perisian,bersama-sama dengan semua maklumat dan parameter, prosedur, butiran konfigurasi dan perisian sokongan yang diperlukan sebagai langkah luar jangka (contigency), dan selagi perisian itu diperlukan untuk membaca atau memproses data yang diarkibkan.	

ID	KETERANGAN	PERANAN
4.20 Keselamatan Rangkaian		
4.20.1	**Keselamatan Rangkaian** Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi termasuk: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah dipasang di dalam rak di bilik *server* / bilik komunikasi yang disediakan. Pemasangan mesti dibuat dengan kemas dan teratur termasuk peralatan, sistem pengkabelan dan punca kuasa yang bersesuaian. Sistem pendawaian kabel data bagi pengguna mesti dipasang dari bilik *server* / bilik komunikasi ke bilik / meja pegawai. (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan mestilah melalui proses *Factory Acceptance Test* (FAT) sebelum pemasangan dan konfigurasi dan proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;	ICTSO Pengurus ICT Pentadbir Keselamatan ICT Pentadbir Rangkaian ICT

ID	KETERANGAN	PERANAN
	(e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Keselamatan ICT; (f) Semua laluan keluar dan masuk hendaklah melalui *firewall* di bawah kawalan LHDNM; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang di pasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; (h) Memasang perkakasan dan perisian yang bersesuaian seperti *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat LHDNM; (i) Memasang *Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan ke rangkaian yang bukan di bawah kawalan LHDNM adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian LHDNM sahaja di mana penggunaan modem adalah dilarang sama sekali; (l) Kemudahan bagi *wireless* LAN yang dibenarkan perlu dilaksanakan dan menepati keperluan keselamatan ICT;	

ID	KETERANGAN	PERANAN
	(m) Memasang perkakasan dan perisian *Bandwidth Management System* bagi memastikan pengurusan sistem rangkaian dapat memberi keutamaan mengikut keperluan; (n) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; (o) Menempatkan atau memasang antara muka (interfaces) yang bersesuaian diantara rangkaian LHDNM, rangkaian agensi lain dan rangkaian awam; (p) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna 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 LHDNM; dan (t) Mewujud dan melaksana kawalan pengalihan laluan (routing control) bagi memastikan pematuhan terhadap peraturan LHDNM.	

ID	KETERANGAN	PERANAN
4.21 Keselamatan Perkhidmatan Rangkaian		
4.21.1	**Keselamatan Perkhidmatan Rangkaian** Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian LHDNM, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO Pengurus ICT Pentadbir Keselamatan ICT Pentadbir Rangkaian ICT Pentadbir Sistem ICT
4.22 Pengasingan Rangkaian		
4.22.1	**Pengasingan Rangkaian** Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian LHDNM. Pengasingan perkhidmatan rangkaian bertujuan meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara–perkara yang perlu dipatuhi adalah:	ICTSO Pengarah Bahagian Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	(a) Melaksanakan konfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; (b) Menyediakan rangkaian terasing (isolated network) untuk orang luar atau pelawat yang hadir ke pejabat LHDNM dan memerlukan capaian Internet. Rangkaian ini hendaklah tidak dibenarkan mengakses rangkaian dalaman LHDNM dan perlu dipantau dari semasa ke semasa. (c) Mengemaskini hak capaian pengguna dari semasa ke semasa mengikut keperluan.	
4.23 Penapisan Web		
4.23.1	**Penapisan Web** Untuk melindungi sistem daripada terjejas oleh perisian berbahaya dan untuk menghalang akses kepada web yang tidak dibenarkan. LHDNM bertanggungjawab mengurangkan risiko kakitangan mengakses laman web yang tidak dibenarkan dan mengandungi maklumat yang tidak diketahui kesahihannya atau mengandungi virus dan cubaan untuk mendapatkan maklumat peribadi dengan cara manipulasi, memberi tekanan dan memperdaya (phishing) kakitangan. LHDNM perlu mengesan dan menyekat alamat IP dan domain laman web yang diragui untuk mengawal akses kepada kandungan yang mungkin tidak sesuai	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	atau berpotensi membahayakan pengguna terutamanya dalam persekitaran organisasi kerajaan.	
4.24 Penggunaan Kriptografi		
4.24.1	**Penyulitan Data (Enkripsi)** Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi semasa dalam storan dan penghantaran mengikut keperluan dan infrastruktur teknologi semasa.	Pengurus ICT Pentadbir Sistem ICT Pemilik Sistem ICT Warga Hasil Pihak Ketiga
4.24.2	**Tandatangan Digital** Penggunaan tandatangan digital adalah perlu kepada pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pengurus ICT Pentadbir Sistem ICT Pemilik Sistem ICT Warga Hasil Pihak Ketiga
4.24.3	**Pengurusan Infrastruktur Kunci Awam (PKI)** Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pengurus ICT Pentadbir Sistem ICT Pemilik Sistem ICT Warga Hasil Pihak Ketiga
4.25 Kitaran Hayat Pembangunan Sistem Yang Selamat		
4.25.1	**Kitaran Hayat Pembangunan Sistem Yang Selamat** Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk	ICTSO Pengarah Bahagian

ID	KETERANGAN	PERANAN
	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 mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	Pentadbir Sistem ICT
4.26 Keperluan Keselamatan Sistem Maklumat		
4.26.1	**Analisis Keperluan dan Spesifikasi Keselamatan Maklumat** Pembangunan sistem baharu atau penambahbaikan sistem sedia ada hendaklah mematuhi perkara-perkara berikut: (a) Semua sistem yang dibangunkan sama ada secara dalaman atau khidmat luaran hendaklah dikaji supaya mengikut keperluan	Pentadbir Sistem ICT Pembekal

ID	KETERANGAN	PERANAN
	pengguna dan selaras dengan dasar atau peraturan semasa yang berkuat kuasa seperti Panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA) dan *Enterprise Architecture* Sektor Awam (EA); (b) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan; (c) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber LHDNM; (d) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; (e) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang ditetapkan; dan (f) Ujian keselamatan hendaklah dilakukan di setiap peringkat pembangunan sistem bagi memastikan integriti data.	

ID	KETERANGAN	PERANAN
4.26.2	**Melindungi Perkhidmatan Aplikasi Dalam Rangkaian Awam** Maklumat aplikasi yang melalui rangkaian awam hendaklah dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat, pengubahsuaian maklumat yang tidak dibenarkan dan pertikaian kontrak. Perkara-perkara yang perlu dipatuhi adalah: (a) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; (b) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; (c) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan MFA (Multi Factor 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	CDO Pentadbir Sistem ICT Pembekal

ID	KETERANGAN	PERANAN
	penghantaran serta penerimaan dokumen dan kontrak.	
4.26.3	**Melindungi Transaksi Perkhidmatan Aplikasi** 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.	CDO Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
4.27 Prinsip Rekabentuk dan Kejuruteraan Sistem Yang Selamat		
4.27.1	**Prinsip Kejuruteraan Sistem Yang Selamat** 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. Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut : (a) Proses pengemaskinian perisian atau sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan; (c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; (d) Mengawal capaian ke atas kod atau cara program bagi mengelakkan kerosakan,	Pentadbir Sistem ICT Pembangun Sistem

ID	KETERANGAN	PERANAN
	pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (e) Data ujian perlu dipilih dengan berhatihati, dilindungi dan dikawal; dan (f) Semua sistem konfigurasi perlu didaftardan didokumenkan.	
4.28 Pengaturcaraan Program Selamat		
4.28.1	**Pengaturcaraan Program Selamat** Kawalan capaian kepada kod sumber atau atur cara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran. Kod sumber bagi semua aplikasi dan perisian ialah hak milik Kerajaan.	Pentadbir Sistem ICT Pembangun Sistem Pengurus Projek
4.29 Pengujian Keselamatan dan Penerimaan Sistem		
4.29.1	**Pengujian Keselamatan Sistem** 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 ICT

ID	KETERANGAN	PERANAN
	(b) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan (c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	
4.29.2	**Pengujian Penerimaan Sistem** Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang periu dipatuhi adalah seperti yang berikut: (a) Pengujian penerimaan sistem hendaklah merangkumi Keperluan keselamatan sistem maklumat dan kepatuhan kepada polisi pembangunan selamat; (b) Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan (c) Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (vulnerability scanner).	ICTSO Pentadbir Sistem ICT Pengguna

ID	KETERANGAN	PERANAN
	Maklumat lanjut berkaitan boleh merujuk kepada dokumen ISO/IEC/IEEE 29119 Software Testing Standard.	
4.30 Pembangunan Penyumberan Luar		
4.30.1	**Pembangunan Oleh Sumber Luar** LHDNM hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (source code) adalah menjadi HAK MILIK LHDNM. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Perkiraan perlesenan, kod sumber ialah HAK MILIK LHDNM dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*; (b) Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko"; (c) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian	ICTSO Pengarah Bahagian Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; (d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; (e) Mengguna pakai prinsip dan tatacara *escrow*; dan (f) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.	
4.31 Pengasingan Persekitaran Pembangunan, Pengujian Dan Produksi		
4.31.1	**Pengasingan Persekitaran Pembangunan, Pengujian Dan Produksi** Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepadapersekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (production).	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	(b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan (c) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.	
4.32 Pengurusan Perubahan		
4.32.1	**Pengurusan Perubahan** Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara 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 mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	
4.33 Data Pengujian		
4.33.1	**Perlindungan Data Ujian** Data pengujian hendaklah dipilih, dilindungi dan diuruskan dengan sewajarnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji dan disahkan; (c) Pengujian perisian perlu dilakukan di dalam persekitaran yang berasingan dari pembangunan dan produksi;	Pentadbir Keselamatan ICT Pentadbir Rangkaian ICT Pentadbir Sistem ICT Pemilik Sistem ICT

ID	KETERANGAN	PERANAN
	(d) Mengawal capaian ke atas kod atau aturcara bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (e) Data ujian perlu memenuhi keperluan sistem, dilindungi dan dikawal; (f) Mengaktifkan audit log bagi merekodkan aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan mengikut keperluan; dan (g) Akses kepada *source code* aplikasi perlu dihadkan kepada pengguna yang dibenarkan.	
4.34 Perlindungan Sistem Maklumat Semasa Pelaksanaan Audit		
4.34.1	**Kawalan Audit Sistem Maklumat** Pelaksanaan audit dan jaminan aktiviti melibatkan penilaian operasi sistem hendaklah dirancang dan dipersetujui antara penguji dan pengurusan yang sesuai. 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 ICT Pengguna

ID	KETERANGAN	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.	

Lampiran A

UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di LHDNM:

(a) Akta Cukai Pendapatan 1967;
(b) Polisi Keselamatan Siber Jabatan Digital Negara Versi 1.0;
(c) Surat Pekeliling Am Bil. 8 Tahun 2024 – Garis Panduan Pengurusan Dan Pengendalian Rahsia Rasmi Dalam Perkhidmatan Awam;
(d) Arahan Keselamatan LHDN Bil. 1 Tahun 2004 – Kawalan Keluar Masuk Barang-Barang Di Bangunan / Kawasan Lembaga Hasil Dalam Negeri;
(e) Garis Panduan Pengurusan Aset (GPPA) LHDNM – PK BIL 9/2023;
(f) Garis Panduan Pengurusan Aset (Pindaan 2023);
(g) Pekeliling Am Bilangan 3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
(h) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
(i) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 : Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
(j) Surat Pekeliling Am Bilangan 3 Tahun 2024 : Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
(k) Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022;
(l) Surat Arahan Ketua Setiausaha Negara – Langkah-langkah untuk memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-Agensi Kerajaan (20 Oktober 2006);
(m) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan (1 Jun 2007);
(n) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di AgensiAgensi Kerajaan (23 November 2007);

(o) Surat Pekeliling Perbendaharaan Bil. 2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

(p) Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan;

(q) Pekeliling Perkhidmatan Lembaga Hasil Dalam Negeri Malaysia Bil. 5/2005 Mengenai Dasar Latihan Sumber Manusia;

(r) PK 2.6: Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam;

(s) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam;

(t) Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan dalam Perkhidmatan Awam;

(u) Akta Tandatangan Digital 1997;

(v) Akta Rahsia Rasmi 1972;

(w) Pekeliling Am Bilangan 2 Tahun 1987 Garis Panduan Mengenai Pengelasan Fail;

(x) Akta Jenayah Komputer 1997;

(y) Akta Hakcipta (Pindaan) 1997;

(z) Akta Komunikasi dan Multimedia 1998;

(aa) Perintah-Perintah Am;

(bb) Arahan Perbendaharaan;

(cc) Arahan Teknologi Maklumat 2007;

(dd) Garis Panduan Keselamatan MAMPU 2004;

(ee) Akta Arkib Negara;

(cc) Dasar Keselamatan Perlindungan Lembaga Hasil Dalam Negeri Malaysia;

(dd) Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional.

Lampiran 1A

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER LHDNM
(PEKERJA LHDNM)

Nama	:	……
No. Kad Pengenalan	:	……
Jawatan	:	……
Sektor/Jab/Caw.Khas/HASiL Negeri	:	……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber LHDNM; dan

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

.....

(Tandatangan Pegawai)

Sektor/Jab/Caw.Khas/HASiL Negeri

Nama : .....

No.KP: .....

Tarikh : .....

Lampiran 1B

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER LHDNM
(PIHAK KETIGA)

Nama : ……

No. Kad Pengenalan : ……

Nama Syarikat : ……

Alamat 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 LHDNM; dan

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

…… ……

(Tandatangan Wakil Syarikat) (Tandatangan Saksi)

Nama : ..... Nama : .....

No. KP : ..... No. KP : .....

Tarikh : ..... Tarikh : .....

Pengesahan Pegawai LHDNM

.....

(Nama Pegawai LHDNM)

b.p Ketua Pegawai Eksekutif / Ketua Pengarah Hasil Dalam Negeri

Tarikh : .....

Lampiran 2

RAJAH 1: RINGKASAN PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT LHDNM