LEMBAGA LEBUHRAYA MALAYSIA

POLISI KESELAMATAN SIBER

23 Mei 2024

Versi 1.0

BAHAGIAN TEKNOLOGI MAKLUMAT

LEMBAGA LEBUHRAYA MALAYSIA

2024

Penasihat

YBhg. Dato' Ir. Sazali Bin Harun
Ketua Pengarah
Lembaga Lebuhraya Malaysia

Penyelaras

Puan Norzuriati binti Zainol Rashid
Pengarah Bahagian Teknologi Maklumat
Lembaga Lebuhraya Malaysia

KATA-KATA ALUAN KETUA PENGARAH LEMBAGA LEBUHRAYA MALAYSIA

Terlebih dahulu saya ingin mengucapkan tahniah kepada Bahagian Teknologi Maklumat di atas kejayaan menghasilkan penerbitan bertajuk Polisi Keselamatan Siber Lembaga Lebuhraya Malaysia (LLM) untuk dijadikan rujukan khasnya oleh warga LLM.

Adalah menjadi hasrat kerajaan untuk meningkatkan keberkesanan sistem penyampaian melalui penggunaan ICT. Selaras dengan hasrat ini, LLM telah meningkatkan penggunaan ICT dalam meningkatkan kualiti penyampaian perkhidmatan dengan menyediakan lebih banyak saluran interaktif yang terkini untuk digunakan.

Sejajar dengan kemajuan teknologi maklumat dan era dunia tanpa sempadan pada hari ini, kita tidak dapat lari daripada ancaman siber seperti pencerobohan data, *fraud* dan sebagainya. Sehubungan itu, adalah penting untuk kita selaku pengguna ICT memahami dan mengetahui kaedah serta prosedur tertentu dalam menggunakan aplikasi ICT secara berhemah yang seterusnya dapat mengurangkan risiko daripada terdedah kepada pelbagai bentuk ancaman seperti yang dinyatakan.

Sebagai memenuhi hasrat ini, penerbitan dokumen Polisi Keselamatan Siber diharap dapat dijadikan panduan oleh semua warga LLM di samping memberi pendedahan mengenai kaedah penggunaan ICT yang selamat dan penerangan mengenai bahaya ancaman ICT terhadap operasi LLM.

Justeru, saya menyeru kepada semua warga LLM agar dapat menggunakan peralatan ICT dengan bijak dan berhemah serta mematuhi arahan-arahan keselamatan yang terkandung dalam Polisi Keselamatan Siber Lembaga Lebuhraya Malaysia.

Terima kasih.

YBhg. Dato' Ir. Sazali bin Harun

KATA-KATA ALUAN PENGARAH BAHAGIAN TEKNOLOGI MAKLUMAT

Assalamualaikum dan salam sejahtera.

Alhamdulillah segala puji bagi Allah di atas IzinNya julung kali Bahagian Teknologi Maklumat (BTM) berjaya mengeluarkan satu polisi mengenai keselamatan ICT yang dikenali sebagai Polisi Keselamatan Siber LLM.

Polisi ini akan menjadi rujukan kepada semua warga LLM dalam pengurusan dan pelaksanaan ICT yang berkaitan dengan isu-isu keselamatan perkakasan, perisian dan juga maklumat. Kemajuan teknologi ICT yang begitu pesat berkembang masa kini sangat memberi kesan kepada sistem penyampaian perkhidmatan kerajaan. Soal keselamatan ICT terutamanya serangan siber perlu diambil perhatian yang serius. Ancaman siber ini semakin giat aktif pada masa kini amat berbahaya apabila perkara ini berlaku diluar kawalan fisikal di mana ia menerusi jaringan rangkaian awam (internet) yang terdedah kepada umum.

Justeru, dengan adanya Polisi Keselamatan Siber ini maka setiap pengguna ICT di LLM akan lebih berhati-berhati dan sentiasa merujuk kepada langkah-langkah keselamatan yang tertera dalam polisi ini. Pematuhan kepada keselamatan seperti yang terkandung dalam Polisi Keselamatan Siber ini adalah wajib dipatuhi dan sebarang penyelewengan boleh menyebabkan seseorang pegawai atau kakitangan diambil tindakan yang sewajarnya. Oleh itu saya menyeru kepada semua warga LLM agar mematuhi segala peraturan keselamatan ICT yang telah digariskan agar pelaksanaan program ICT di LLM berjaya mencapai matlamat yang dtetapkan dan selamat daripada sebarang insiden keselamatan ICT.

Akhir kata, setinggi-tinggi penghargaan dan ucapan tahniah saya rakamkan kepada semua pegawai dan kakitangan yang telah terlibat secara langsung atau tidak langsung dalam usaha penerbitan Polisi Keselamatan Siber LLM ini.

Terima Kasih.

“Keselamatan Tanggungjawab Bersama”

Puan Norzuriati binti Zainol Rashid

ISI KANDUNGAN

1.0 GLOSARI / TERMA RUJUKAN

(1)	Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
(2)	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
(3)	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.
(4)	*Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
(5)	Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
(6)	*Bandwidth*	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
(7)	BCP/PKPn	*Business Continuity Planning* Pelan Kesinambungan Perkhidmatan
(8)	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.
(9)	CIA	*Confidentiality, Integrity, Availability*

(10)	CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi.
(11)	*Clear Desk* dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada ditempatnya.
(12)	*Data-at-rest* (data dalam simpanan)	*Refers to data that is being stored in stable destination systems. Data at rest is frequently defined as data that is not in use or is not traveling to system endpoints, such as mobile devices or workstations*.
(13)	*Data-in-motion* (data dalam pergerakan)	*Refers to stream of data moving through any kind of network. It represents data which is being transferred or moved*.
(14)	*Data-in-use* (data dalam penggunaan)	*Refers to data that is not simply being passively stored in stable destination, such as central data warehouse, but is working its way through other parts of an IT architecture*.
(15)	*Denial of Service*	Halangan pemberian perkhidmatan.
(16)	*Defence-in-depth*	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data atau maklumat.
(17)	*Downloading*	Aktiviti muat turun sesuatu perisian.
(18)	*Encryption*	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.

(19)	*Escrow* (eskrow)	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
(20)	*Firewall*	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
(21)	*Forgery*	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
(22)	CERT LLM	*Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT LLM.
(23)	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
(24)	*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
(25)	ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi.
(26)	ICTSO	ICT *Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
(27)	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akautabiliti.

(28)	Impak fungsi jabatan	Melibatkan perkara-perkara daripada segi kewangan, reputasi, ketidakpatuhan dan pelanggaran privasi.
(29)	Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
(30)	*Internet*	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
(31)	Internet *Gateway*	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
(32)	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan yang hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
(33)	ISDN	*Integrated Services Digital Network* Menggunakan isyarat digital pada talian telefon analog sedia ada.
(34)	*Intrusion Detection System* (IDS)	Sistem Pengesanan 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.

(35)	*Intrusion Prevention System* (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian. dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
(36)	ISMS	*Information Security Management System* Sistem Pengurusan Keselamatan Maklumat
(37)	LLM	Lembaga Lebuhraya Malaysia
(38)	Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman daripada pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
(39)	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin diekspoitasikan dan mengakibatkan pelanggaran keselamatan.
(40)	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (*standard format*) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
(41)	LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
(42)	*Lock*	Mengunci komputer.
(43)	*Logout*	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.

(44)	*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.
(45)	*Mobile Code*	*Mobile code* merupakan perisian yang boleh dipindahkan antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh *Java Applet, ActiveX* dan sebagainya pada pelayar internet.
(46)	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.
(47)	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dngan bayaran yang dipersetujui.
(48)	Pasukan CERT	*Computer Emergency Response Team (CERT)*
(49)	Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan daripada segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa
(50)	Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko

(51)	Perisian Aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* atau pun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
(52)	*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*.
(53)	*Rollback (undur)*	Pengembalian pangkalan data atau program kepada stabil sebelum sesuatu ralat berlaku.
(54)	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian *internet*.
(55)	Ruang Siber	Sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT.
(56)	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ia tidak digunakan dalam jangka masa tertentu.
(57)	*Server*	Pelayan Komputer

(58)	*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.
(59)	*Switch*	*Switch* merupakan gabungan hab (*hub*) dan jambatan (*bridge*) yang menapis bingkai (*frame*) supaya mensegmenkan rangkaian. Kegunaan *switch* dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu sistem penghantaran dengan mengurangkan perlanggaran yang berlaku.
(60)	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
(61)	*Uninterruptible Power Supply* (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
(62)	*Video Conference*	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa yang sama ia diterima oleh penghantar.
(63)	*Video Streaming*	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
(64)	*Virus*	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
(65)	WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.

(66)	Warga LLM	Kakitangan kerajaan yang berkhidmat di LLM sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT LLM.
(67)	*Wireless* LAN	Jaringan komputer yang berhubung tanpa melalui kabel.
(68)	*Worm*	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

2.0 TUJUAN

Polisi Keselamatan Siber (PKS), Lembaga Lebuhraya Malaysia (LLM) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga LLM, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM dalam melindungi maklumat di ruang siber.

Polisi Keselamatan Siber LLM mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Lembaga Lebuhraya Malaysia (LLM). Polisi ini juga menerangkan kepada semua pengguna di LLM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT LLM. Aset ICT termasuk data, maklumat, perkakasan, perisian, aplikasi, rangkaian, dokumentasi dan kemudahan ICT yang berada di bawah tanggungjawab LLM.

3.0 LATAR BELAKANG

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

4.0 OBJEKTIF

Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti yang berikut:

(i) Menerangkan kepada semua pengguna merangkumi warga LLM, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber.

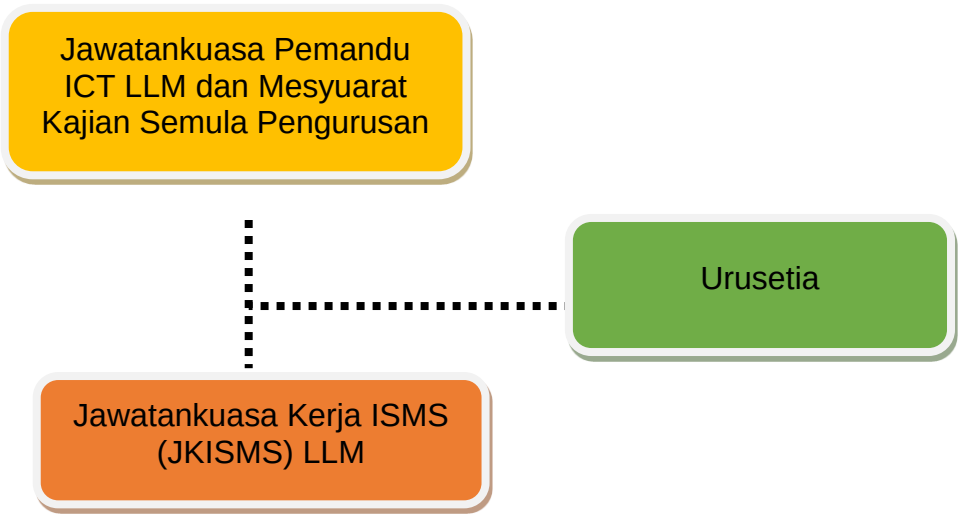
(ii) Memastikan keselamatan penyampaian perkhidmatan LLM di tahap tertinggi dan meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

(iii) Memastikan kelancaran operasi LLM dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

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

(v) Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT

5.0 TADBIR URUS



Rajah 1: Struktur Jawatankuasa Pemandu ICT, Mesyuarat Kajian Semula Pengurusan dan Jawatankuasa Kerja ISMS LLM

(i) Keahlian JPICT/ Mesyuarat Kajian Semula Pengurusan ini adalah seperti yang berikut:

Pengerusi: Ketua Pengarah LLM

Ahli:

i. Pengurusan LLM;

ii. Semua Pengarah Bahagian;

iii. Penolong Wakil Pengurusan;

iv. ICTSO LLM.

Urus Setia: Bahagian Teknologi Maklumat (BTM)

(ii) Bidang rujukan JPICT/ Mesyuarat Kajian Semula Pengurusan adalah seperti yang berikut:

a) Menentukan hala tuju keseluruhan pelaksanaan pensijilan ISMS LLM yang merangkumi perancangan, pemantauan dan pengesahan terhadap:

i. Pelaksanaan pensijilan ISMS ke atas perkhidmatan LLM yang dikenal pasti;
ii. Kelulusan ke atas dasar, objektif dan skop pelaksanaan ISMS;
iii. Penetapan kriteria penerimaan risiko, tahap risiko dan pelan penguraian risiko;
iv. Keputusan dan tindakan Mesyuarat Jawatankuasa ISMS;
v. Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik LLM;
vi. Keperluan ISMS diterapkan dalam budaya kerja pegawai LLM;
vii. Sumber yang diperlukan oleh pasukan pelaksana ISMS;
viii. Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya;
ix. Pencapaian sasaran ISMS seperti yang dirancang;
x. Arahan dan sokongan kepada Pasukan ISMS LLM bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan
xi. Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan.

6.0 ASET ICT LLM

Aset ICT LLM merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran seperti berikut:

(i) **Maklumat**

Semua penyedia perkhidmatan dalam LLM hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

(a) Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

(b) Maklumat Rasmi

Maklumat rasmi ialah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh LLM semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

(c) Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (PII atau *Personally Identifiable Information*) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

(d) Data Terbuka

Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. PII dikecualikan daripada data terbuka.

(ii) **Aliran Data**

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

(a) Saluran komunikasi dan aliran data antara sistem di LLM;

(b) Saluran komunikasi dan aliran data ke sistem luar; dan

(c) Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

(iii) **Platform Aplikasi dan Perisian**

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

(iv) **Peranti Fizikal dan Sistem**

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

(a) Pelayan;
(b) Peranti/Peralatan Rangkaian;
(c) Komputer Peribadi/Komputer Riba;
(d) Telefon/peranti pintar;
(e) Media Storan;
(f) Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);

(g) Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan; dan

(h) Peranti pengesahan (*authentication devices*), contohnya token keselamatan, *dongle* dan alat pengimbas biometrik.

(v) **Sistem Luaran**

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

(vi) **Sumber Luaran**

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

(a) Perisian Sebagai Satu Perkhidmatan

(b) Platform Sebagai Satu Perkhidmatan

(c) lnfrastruktur Sebagai Satu Perkhidmatan

(d) Pemulihan Bencana Sebagai Satu Perkhidmatan

(e) Storan Pengkomputeran Awan

(f) Pemantauan Keselamatan

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

7.0 RISIKO

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

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

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

(i) **Kerentanan**

Kerentanan merupakan kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

(ii) **Ancaman**

LLM hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasli.

(iii) **Impak**

LLM hendaklah menganggarkan impak insiden yang mungkin terjadi. lmpak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi LLM.

(iv) **Tahap Risiko**

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

(v) **Penguraian Risiko**

(a) Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

(b) Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

(i) Teknologi

Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, tembok api (*firewall*) digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

(ii) Proses

Perekayasaan (*reengineering*) proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

(iii) Manusia

Mengenal pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

(vi) **Pengurusan Risiko**

(a) Penyedia perkhidmatan digital di LLM hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

(i) Mengenal pasti kerentanan;
(ii) Mengenal pasti ancaman;
(iii) Menilai risiko;
(iv) Menentukan penguraian risiko;
(v) memantau keberkesanan penguraian risiko; dan
(vi) Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

(b) Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan **sekurang-kurangnya sekali setahun** dan dimaklumkan kepada Mesyuarat Jawatankuasa Kerja ISMS, Mesyuarat Jawatankuasa Pemandu ICT atau Mesyuarat Kajian Semula Pengurusan.

8.0 PRINSIP KESELAMATAN

Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, LLM hendaklah melaksanakan prinsip keselamatan seperti yang berikut:

(i) **Prinsip "Perlu-Tahu"**

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

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

(ii) **Hak Keistimewaan Minimum**

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

(iii) **Pengasingan Tugas**

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

(iv) **Kawalan Capaian Berdasarkan Peranan**

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

(v) **Peminimuman Data**

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

9.0 TEKNOLOGI

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

(i) **Peringkat Pemprosesan Data**

(a) Data-dalam-simpanan

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

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

(b) Data-dalam-pergerakan

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

(c) Data-dalam-penggunaan

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

(ii) Teknologi yang bersesuaian boleh digunakan oleh LLM untuk memastikan asal data dan data/transaksi tanpa-sangkal.

(d) Perlindungan Ketirisan Data

(i) Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

(ii) Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

(ii) **Elemen Dalam Persekitaran Pengkomputeran**

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

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

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

(a) Peranti pengkomputeran peribadi

(i) Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet dan peranti storan.

(ii) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada LLM. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat.

(b) Peranti rangkaian

(i) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling berhubung antara peranti komputer dan sistem seperti *switch*, penghala, tembok api, peranti VPN dan kabel.

(c) Aplikasi

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

(ii) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam SPK-ISMS-009 – Penghantaran dan Pertukaran Maklumat.

(d) Pelayan

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

(e) Persekitaran fizikal

(i) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

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

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

10.0 PROSES

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

(i) **Konfigurasi Asas**

(a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.

(b) Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

(ii) **Kawalan Perubahan Konfigurasi**

(a) Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

(b) Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.

(c) Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

(iii) **Sandaran (*Backup*)**

(a) Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.

(b) Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

(iv) **Kitaran Pengurusan Aset**

(i) Pindah

(a) Pemindahan hak milik aset berlaku dalam keadaan berikut:

(i) Warga LLM meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;

(ii) Aset yang dikongsi untuk kegunaan sementara;

(iii) Pemberian aset kepada agensi lain; dan

(iv) Aset dikembalikan setelah tamat tempoh sewaan. Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan.

(ii) Pelupusan

(a) Pelupusan media storan hendaklah dirujuk kepada Jawatankuasa Menyemak, Menilai dan Mengelaskan Semula Rahsia Rasmi sebagai langkah pertama di mana Jawatankuasa Menyemak, Menilai dan Mengelaskan Semula Rahsia Rasmi akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.

(b) Berdasarkan keputusan Jawatankuasa Menyemak, Menilai dan Mengelaskan Semula Rahsia Rasmi, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.

(c) Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.

(d) Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam yang sedang berkuat kuasa.

(iii) Kitaran Hayat

(a) Kitaran hayat data hendaklah diuruskan mengikut Akta 629.

(b) Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

11.0 MANUSIA

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

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

(i) **Kompetensi Pengguna**

(a) Kompetensi pengguna termasuk:

(i) Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber.

(ii) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga LLM berhubung alat-alat keselamatan berkaitan untuk memastikan warga LLM melaksanakan tugas harian mereka.

(b) Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam. Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

(ii) **Kompetensi Pelaksana**

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

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

(i) Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.

(ii) Memenuhi keperluan pembelajaran berterusan.

(iii) Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.

(iv) Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

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

(iii) **Peranan**

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

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

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

(d) Warga LLM yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.

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

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

12.0 PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Setiap projek di LLM hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.

Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), Polisi Keselamatan Siber LLM dan surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.

Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.

Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap peranti pengkomputeran peribadi, peranti rangkaian, aplikasi, pelayan dan persekitaran fizikal.

13.0 PERNYATAAN POLISI KESELAMATAN SIBER LLM

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

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

(i) **Kerahsiaan**
Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

(ii) **Integriti**
Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan.

(iii) **Tidak Boleh Disangkal**
Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

(iv) **Kesahihan**
Data dan maklumat hendaklah dipastikan kesahihannya.

(v) **Ketersediaan**
Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT LLM, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

14 bidang keselamatan yang terlibat di dalam Polisi Keselamatan Siber LLM diterangkan dengan lebih jelas dan teratur seperti berikut:

BIDANG A.1

POLISI KESELAMATAN MAKLUMAT

(*INFORMATION SECURITY POLICY*)

A1.1 Hala Tuju Pengurusan Untuk Keselamatan Maklumat *(Management Directions for Information Security)*

A.1.1.1 Polisi Keselamatan Maklumat

(Policies for Information Security)

A1.1.2 Kajian Semula Polisi untuk Keselamatan Maklumat

(Review of Policies for Information Security

A.1.1 HALA TUJU PENGURUSAN UNTUK KESELAMATAN MAKLUMAT (*MANAGEMENT DIRECTIONS FOR INFORMATION SECURITY*)

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

A.1.1.1 Polisi Keselamatan Maklumat (*Policies for Information Security*)

Peranan: JPICT/CIO/ ICTSO/ Pengarah Bahagian

Pelaksanaan polisi ini akan dijalankan oleh Ketua Pengarah LLM dengan disokong oleh Jawatankuasa Pemandu ICT / Mesyuarat Kajian Semula Pengurusan / JKISMS yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), Pengarah Bahagian dan ahli-ahli yang dilantik oleh Ketua Pengarah LLM.

Polisi Keselamatan Siber LLM mestilah dipatuhi oleh semua warga LLM, Syarikat Konsesi, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM.

Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan LLM kepada warga LLM, pembekal, perunding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM.

Polisi ini dimuktamadkan menerusi kelulusan Jawatankuasa Pemandu ICT (JPICT) LLM.

A.1.1.2 Kajian Semula Polisi untuk Keselamatan Maklumat (*Review of Policies for Information*)

Peranan: JPICT/CIO/ICTSO

Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundanga dan polisi Kerajaan. Berikut ialah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber LLM:

i. Mengenal pasti dan menentukan perubahan yang diperlukan;
ii. Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan;
iii. Memaklumkan pindaan yang telah disahkan oleh JPICT kepada warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM; dan
iv. Polisi ini hendaklah dikaji semula **setiap LIMA (5) TAHUN SEKALI** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.

BIDANG A.2

PERANCANGAN BAGI KESELAMATAN ORGANISASI

(*ORGANIZATION OF INFORMATION SECURITY*)

A.2.1 Perancangan Dalaman

(Internal Organization)

A.2.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat

(The Role and Responsibility of Information Security)

A.2.1.2 Pengasingan Tugas

(Segregation of Duties)

A.2.1.3 Hubungan Dengan Pihak Berkuasa

(Contact with Authorities)

A.2.1.4 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus

(Contact with Special Interest Groups)

A.2.1.5 Keselamatan Maklumat dalam Pengurusan Projek

(Information Security in Project Management)

A.2.2.2 Peranti Mudah Alih dan Telekerja

(Mobile Devices and Teleworking)

A.2.2.1 Polisi Peranti Mudah Alih

(Mobile Device Policy)

A.2.2.2 Telekerja

(Teleworking)

A.2.1 PERANCANGAN DALAMAN (*INTERNAL ORGANIZATION*)

Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber LLM.

A.2.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat (*The Role and Responsibility of Information Security*)

(i) **Ketua Pengarah**

Peranan: Ketua Pengarah

Peranan dan tanggungjawab adalah seperti yang berikut:

(a) Memastikan penguatkuasaan pelaksanaan Polisi ini;

(b) Memastikan warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital LLM memahami dan mematuhi peruntukan- peruntukan di bawah Polisi ini;

(c) Memastikan semua keperluan LLM seperti sumber kewangan, sumber manusia dan perlindungan keselamatan adalah mencukupi;

(d) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini;

(e) Mempengerusikan Mesyuarat JPICT LLM; dan

(f) Melantik CIO dan ICTSO.

(ii) **Ketua Pegawai Maklumat (CIO)**

Peranan: CIO LLM

Peranan dan tanggungjawab CIO adalah seperti yang berikut:

(a) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam Polisi ini;

(b) Memastikan kawalan keselamatan maklumat dalam LLM diseragam dan diselaraskan dengan sebaiknya;

(c) Memastikan Pelan Strategik Pendigitalan ICT LLM mengandungi aspek keselamatan siber; dan

(d) Menyelaras pelan latihan dan program kesedaran keselamatan siber.

(iii) **Pegawai Keselamatan ICT (ICTSO)**

Peranan: ICTSO

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti yang berikut:

(a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini;

(b) Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat yang berkuat kuasa;

(c) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

(d) Melaporkan insiden keselamatan siber kepada CERT LLM dan seterusnya membantu dalam penyiasatan atau pemulihan;

(e) Melaporkan insiden keselamatan siber kepada CIO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKPn);

(f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera;

(g) Melaksanakan pematuhan Polisi ini oleh warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM;

(h) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; dan

(i) Menyedia dan merangka latihan dan program kesedaran keselamatan siber.

(iv) **Pengarah Teknologi Maklumat**

Peranan: Pengarah Teknologi Maklumat

Peranan dan tanggungjawab Pengarah Bahagian ialah melaksanakan keperluan Polisi ini dalam operasi semasa seperti yang berikut:

(a) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru;
(b) Pembelian atau peningkatan perisian dan sistem komputer;
(c) Perolehan teknologi dan perkhidmatan komunikasi baru;
(d) Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan
(e) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa.

(v) **Pentadbir Sistem ICT**

Peranan: Pentadbir Sistem ICT

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti yang berikut:

(a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
(b) Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini;
(c) Memantau aktiviti capaian sistem aplikasi;
(d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta;
(e) Menyimpan rekod jejak audit;
(f) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel dalam keadaan yang baik.

(vi) **Jawatankuasa Pemandu ICT (JPICT)**

Peranan: JPICT LLM

Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil 7 Tahun 2024 ialah merancang dan menentukan langkah - langkah keselamatan siber.

(vii) **Jawatankuasa Teknikal ICT (JTICT) LLM**

Peranan: JTICT LLM

(a) JTICT LLM merupakan jawatankuasa yang bertanggungjawab untuk menilai dan menyokong aspek teknikal bagi keperluan dan keselamatan ICT Bahagian LLM.

(b) JTICT LLM dipengerusikan oleh Pengarah Kanan Pengurusan dengan keahlian terdiri daripada wakil Pengarah Bahagian LLM dan wakil bahagian yang dikenal pasti dan diurus setia oleh PKP.

(c) Peranan dan tanggungjawab JTICT seperti yang terkandung dalam Surat Pekeliling Am Bil 7 Tahun 2024 ialah merancang dan menentukan langkah-langkah keselamatan siber.

(viii) **Jawatankuasa Pemandu ICT/ Mesyuarat Kajian Semula Pengurusan**

Peranan: Jawatankuasa Pemandu ICT/ Mesyuarat Kajian Semula Pengurusan

Bidang rujukan Jawatankuasa Pemandu ICT/ Mesyuarat Kajian Semula Pengurusan adalah seperti yang berikut:

(a) Menentukan hala tuju keseluruhan pelaksanaan pensijilan ISMS LLM yang merangkumi perancangan, pemantauan dan pengesahan terhadap:

(b) Pelaksanaan pensijilan ISMS ke atas perkhidmatan LLM yang dikenal pasti;

(c) Kelulusan ke atas dasar, objektif dan skop pelaksanaan ISMS;

(d) Penetapan kriteria penerimaan risiko, tahap risiko dan risk treatment plan;

(e) Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan LLM yang dikenal pasti;

(f) Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik LLM;

(g) Keperluan ISMS diterapkan dalam budaya kerja pegawai LLM;

(h) Sumber yang diperlukan oleh pasukan pelaksana ISMS;

(i) Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya;

(j) Pencapaian sasaran ISMS seperti yang dirancang;

(k) Arahan dan sokongan kepada Pasukan ISMS LLM bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan

(l) Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan.

Meluluskan:

(a) Struktur organisasi ISMS LLM; dan

(b) Keperluan sumber.

(ix) **Computer Emergency Response Team (CERT) LLM**

Peranan: CERT LLM

Peranan dan tanggungjawab CERT LLM adalah seperti yang berikut:

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

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

(c) Menangani tindak balas insiden keselamatan siber dan mengambil tindakan baik pulih minimum;

(d) Menasihati Pentadbir Sistem/Pelayan untuk mengambil tindakan pemulihan dan pengukuhan; dan

(e) Menyebarkan makluman berkaitan pengukuhan keselamatan siber kepada Pentadbir Sistem ICT.

(x) **Pengguna**

Peranan: Pengguna

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

(a) Membaca, memahami dan mematuhi Polisi ini;

(b) Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya;

(c) Menjalani tapisan keselamatan sekiranya diperlukan dan dikehendaki berurusan dengan maklumat rasmi terperingkat;

(d) Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan;

(i) Melaksanakan langkah-langkah perlindungan seperti yang berikut:

(a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;

(c) Menentukan maklumat sedia untuk digunakan;

(d) Menjaga kerahsiaan maklumat;

(e) Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan;

(f) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

(g) Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum.

(ii) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CERT LLM dengan segera;

(iii) Menghadiri program-program kesedaran mengenai keselamatan siber; dan

(iv) Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini.

A.2.1.2 Pengasingan Tugas (*Segregation of Duties*)

Peranan: Pengarah Bahagian

Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;

(ii) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi;

(iii) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*; dan

(iv) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

A.2.1.3 Hubungan Dengan Pihak Berkuasa (*Contact with Authorities*)

Peranan : ERT LLM dan CERT LLM

Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara- perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab LLM;

(ii) Mewujud dan mengemas kini prosedur / senarai pihak berkuasa perundangan / pihak yang 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

(iii) Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden dan tidak berkompromi kepada sebarang aktiviti pelanggaran.

A.2.1.4 Hubungan Dengan Kumpulan Berkepentingan yang Khusus (*Contact with Special Interest Groups*)

Peranan : Warga LLM (Mengikut Bidang Kepakaran)

Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional ataupun forum bagi:

(i) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;

(ii) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini;

(iii) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan

(iv) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

A.2.1.5 Keselamatan Maklumat dalam Pengurusan Projek (*Information Security in Project Management*)

Peranan : Warga LLM (Pasukan Projek)

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek LLM;

(ii) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;

(iii) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;

(iv) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek; dan

(v) Pihak pembekal yang mempunyai pensijilan keselamatan maklumat (mengikut keperluan)

A.2.2 PERANTI MUDAH ALIH DAN TELEKERJA (*MOBILE DEVICES AND TELEWORKING*)

Objektif : Memastikan keselamatan telekerja dan penggunaan peralatan mudah alih.

A.2.2.1 Polisi Peranti Mudah Alih (*Mobile Device Policy*)

(i) **Peranan** : Pentadbir Sistem ICT

Membangun serta menyebarkan dasar dan langkah-langkah keselamalan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih.

(ii) **Peranan** : Jawatankuasa Pemandu ICT (JPICT) LLM

Meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga LLM.

(iii) **Peranan** : Warga LLM

(a) Perkara-perkara yang perlu dipatuhi:

(b) Pendaftaran ke atas peralatan mudah alih;

(c) Keperluan ke atas perlindungan secara fizikal;

(d) Kawalan ke atas pemasangan perisian peralatan mudah alih;

(e) Kawalan ke atas versi dan *patches* perisian;

(f) Sekatan ke atas akses perkhidmatan maklumat secara dalam talian;

(g) Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi;

(h) Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan; dan

(i) Peralatan mudah alih hendaklah dipasang dengan perisian keselamatan (*antivirus, antimalware*).

A.2.2.2 Telekerja (*Teleworking*)

Peranan: Warga LLM

Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja.

BIDANG A.3

KESELAMATAN SUMBER MANUSIA (*HUMAN RESOURCE SECURITY*)

A.3.1 Sebelum Perkhidmatan

(*Prior To Employment*)

A.3.1.1 Tapisan Keselamatan

(*Security Screening*)

A.3.1.2 Terma dan Syarat Perkhidmatan

(*Terms and Conditions of Employment*)

A.3.2 Dalam Tempoh Perkhidmatan

(*During Employment*)

A.3.2.1 Tanggungjawab Pengurusan

(*Management Responsibilities*)

A.3.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat

(*Information Security Awareness, Education and Training*)

A.3.2.3 Proses Tatatertib

(*Disciplinary Process*)

A.3.3 Penamatan dan Pertukaran Perkhidmatan

(*Termination and Change of Employment*)

A.3.3.1 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan

(*Termination or Change of Employment Responsibilities*)

A.3.1 SEBELUM PERKHIDMATAN (*PRIOR TO EMPLOYMENT*)

Objektif : Memastikan warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

A.3.1.1 Tapisan Keselamatan (*Security Screening*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Tapisan keselamatan hendaklah dijalankan terhadap warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan

(ii) Menjalankan tapisan keselamatan untuk warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

A.3.1.2 Terma dan Syarat Perkhidmatan (*Terms and Conditions of Employment*)

Peranan: Ketua Jabatan, Pentadbir Sistem, Pengguna dan Pembekal

Persetujuan berkontrak dengan warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

(i) Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM yang terlibat dalam menjamin keselamatan aset ICT; dan

(ii) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

A.3.2 DALAM TEMPOH PERKHIDMATAN (*DURING EMPLOYMENT*)

Objektif : Memastikan warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

A.3.2.1 Tanggungjawab Pengurusan (*Management Responsibilities*)

Peranan : Warga, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan LLM

Pengurusan hendaklah memastikan warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.

A.3.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat (*Information Security Awareness, Education and Training*)

Peranan : Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber LLM, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;

(ii) Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber LLM perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan

(iii) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

A.3.2.3 Proses Tatatertib (*Disciplinary Process*)

Peranan : Unit Integriti

Proses tatatertib yang formal dan disampaikan kepada warga LLM hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga LLM yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga LLM sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh LLM;

(ii) Warga LLM yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT LLM

A.3.3 PENAMATAN DAN PERTUKARAN PERKHIDMATAN (*TERMINATION AND CHANGE OF EMPLOYMENT*)

Objektif: Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas diurus dengan teratur.

A.3.3.1 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan (*Termination or Change of Employment Responsibilities*)

Peranan: BSMK dan warga LLM

Warga LLM yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut:

(i) Memastikan semua aset ICT dikembalikan kepada LLM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

(ii) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan LLM dan/atau terma perkhidmatan yang ditetapkan.

(iii) Maklumat rasmi LLM dalam peranti tidak dibenarkan dibawa keluar dari LLM.

Warga LLM yang telah bertukar perkhidmatan hendaklah:

(i) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada LLM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

(ii) Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.

BIDANG A.4 :

PENGURUSAN ASET (*ASSET MANAGEMENT*)

A.4.1 Tanggungjawab Terhadap Aset

(*Responsibility for Assets*)

A.4.1.1 Inventori Aset

(*Inventory of Assets*)

A.4.1.2 Pemilikan Aset

(*Ownership of Assets*)

A.4.1.3 Penggunaan Aset yang Dibenarkan

(*Acceptable Use of Assets*)

A.4.1.4 Pemulangan Aset

(*Return of Assets*)

A.4.2 Pengelasan Maklumat

(*Classification of Information*)

A.4.2.1 Pengelasan Maklumat

(*Classification of Information*)

A.4.2.2 Pelabelan Maklumat

(*Labelling of Information*)

A.4.2.3 Pengendalian Aset

(*Handling of Assets*)

A.4.3 Pengendalian Media

(*Media Handling*)

A.4.3.1 Pengurusan Media Boleh Alih

(*Management of Removal Media*)

A.4.3.2 Pelupusan Media

(*Disposal of Media*)

A.4.3.3 Pemindahan Media Fizikal

(*Physical Media Transfer*)

A.4.1 TANGGUNGJAWAB TERHADAP ASET (*RESPONSIBILITY FOR ASSETS*)

Objektif: Untuk mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT LLM.

A.4.1.1 Inventori Aset (*Inventory of Assets*)

Peranan: Pegawai Penerima Aset, Pegawai Aset dan Warga LLM

Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT LLM. Aset-aset ICT LLM hendaklah diuruskan mengikut Tatacara Pengurusan Aset yang berkuatkuasa.

(i) LLM hendaklah mengenal pasti Pegawai Penerima Aset setiap bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT.

(ii) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumal aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa.

(iii) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja.

(iv) Pegawai Aset hendaklah mengesahkan penempatan aset ICT.

A.4.1.2 Pemilikan Aset (*Ownership of Assets*)

Peranan: Pegawai Aset dan Warga LLM

Aset yang boleh diselenggara hanyalah aset hak milik LLM. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut:

(i) Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset.

(ii) Memastikan aset telah dikelaskan dan dilindungi.

(iii) Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan.

(iv) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan.

(v) Memastikan semua jenis aset dipelihara dengan baik.

A.4.1.3 Penggunaan Aset yang Dibenarkan (*Acceptable Use of Assets*)

Peranan: Warga LLM

Warga LLM hendaklah memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.

A.4.1.4 Pemulangan Aset (*Return of Assets*)

Peranan: Warga LLM

Warga LLM hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.

A.4.2 PENGELASAN MAKLUMAT (*CLASSIFICATION OF INFORMATION*)

Objektif: Untuk mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT LLM.

A.4.2.1 Pengelasan Maklumat (*Classification of Information*)

Peranan: Pegawai Pengelas

Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.

A.4.2.2 Pelabelan Maklumat (*Labelling of Information*)

Peranan: Warga LLM

Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.

A.4.2.3 Pengendalian Aset (*Handling of Assets*)

Peranan: Warga LLM

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:

(i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.
(ii) Memeriksa dan menentukan maklumat adalah 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, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan.

(vii) Memastikan maklumat terperingkat yang disimpan di dalam storan dalaman atau luaran (*internal* atau *external hardisk*) diberi perlindungan melalui kaedah enkripsi yang bersesuaian.

(viii) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

A.4.3 PENGENDALIAN MEDIA (*MEDIA HANDLING*)

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

A.4.3.1 Pengurusan Media Boleh Alih (*Management of Removal Media*)

Peranan: Pentadbir Sistem ICT dan Pengguna

Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh LLM. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:

(i) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat.

(ii) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja.

(iii) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja.

(iv) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan.

(v) Menyimpan semua jenis media di tempat yang selamat.

A.4.3.2 Pelupusan Media (*Disposal of Media*)

Peranan: Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.

Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.

A.4.3.3 Pemindahan Media Fizikal (*Physical Media Transfer*)

Peranan: Warga LLM dan Ketua Jabatan.

Media yang mengandungi maklumat perlu dilindungi daripada akses tanpa izin, penyalahgunaan atau kerosakan semasa dipindahkan. Media yang dimaksudkan juga adalah termasuk dokumen dalam bentuk kertas.

Perkara-perkara berikut perlu dipertimbangkan semasa pemindahan dilakukan seperti berikut:

(i) Perkhidmatan pengangkutan atau kurier yang boleh dipercayai digunakan
(ii) Senarai kurier yang digunakan perlu mendapat persetujuan Ketua Jabatan.
(iii) Pembungkusan perlu mencukupi bagi melindungi kerosakan fizikal yang mungkin timbul semasa transit
(iv) Rekod atau log perlu disimpan untuk mengenalpasti kandungan media, perlindungan yang digunakan serta rakaman semasa pemindahan kepada penjaga transit dan penerimaan di destinasi.

Pemindahan dokumen terperingkat secara fizikal pula perlu mengikut prosedur-prosedur seperti di dalam Arahan Keselamatan.

BIDANG A.5

KAWALAN AKSES (*ACCESS CONTROL*)

A.5.1 Keperluan Kawalan Akses

(*Business Requirements of AccessControl*)

A.5.1.1 Polisi Kawalan Akses

(*Access Control Policy*)

A.5.1.2 Capaian Kepada Rangkaian dan Perkhidmatan Rangkaian

(*Access to Networks and Network Services*)

A.5.2 Pengurusan Akses Pengguna

(*User Access Management*)

A.5.2.1 Pendaftaran dan Pembatalan Pengguna

(*User Registration and Deregistration*)

A.5.2.2 Peruntukan Akses Pengguna

(*User Access Provisioning*)

A.5.2.3 Pengurusan Hak Akses Istimewa

(*Management of Privileged Access Rights*)

A.5.2.4 Pengurusan Maklumat Pengesahan Rahsia Pengguna

(*Management of Secret Authentication Information of Users*)

A.5.2.5 Kajian Semula Hak Akses Pengguna

(*Review of User Access Rights*)

A.5.2.6 Pembatalan atau Pelarasan Hak Akses

(*Removal or Adjustment of Access Rights*)

A.5.3 Tanggungjawab Pengguna

(*User Responsibilities*)

A.5.3.1 Pengurusan Maklumat Pengesahan Rahsia Pengguna

(*Management of Secret Authentication Information of Users*)

A.5.3.2 Penggunaan Maklumat Pengesahan Rahsia

(*Use of Secret Authentication Information*)

A.5.4 Kawalan Akses Sistem dan Aplikasi

(*System and Application Access Control*)

A.5.4.1 Sekatan Akses Maklumat

(*Information Access Restriction*)

A.5.4.2 Prosedur Log Masuk yang Selamat

(*Secure Log-On Procedure*)

A.5.4.3 Sistem Pengurusan Kata Laluan

(*Password Management System*)

A.5.4.4 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa

(*Use of Privileged Utility Programs*)

A.5.4.5 Kawalan Akses Kepada Kod Sumber Program

(*Access Control to Program Source Code*)

A.5.1 KEPERLUAN KAWALAN AKSES (*BUSINESS REQUIREMENTS OF ACCESS CONTROL*)

Objektif: Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.

A.5.1.1 Polisi Kawalan Akses (*Access Control Policy*)

Peranan: Pemilik Perkhidmatan Digital / Pentadbir Sistem ICT

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza.

Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. la perlu dikemas kini setahun sekali atau mengikut keperluan semasa dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Keperluan keselamatan aplikasi;
(ii) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian;
(iii) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa;
(iv) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
(v) Pengasingan peranan kawalan capaian;
(vi) Kebenaran rasmi permintaan akses;
(vii) Keperluan semakan hak akses berkala;
(viii) Pembatalan hak akses; dan
(ix) Keistimewaan akses (*access privilege*).

A.5.1.2 Capaian kepada Rangkaian dan Perkhidmatan Rangkaian (*Access to Networks and Network Services*)

Peranan: ICTSO / Pengarah Teknologi Maklumat / Pentadbir Rangkaian

Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari Pentadbir Rangkaian LLM. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

(i) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian LLM, rangkaian agensi lain dan rangkaian awam;

(ii) Mewujud dan menguatkuasakan mekanisme pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan

(iii) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

A.5.2 PENGURUSAN AKSES PENGGUNA (*USER ACCESS MANAGEMENT*)

Objektif: Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. la perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.

A.5.2.1 Pendaftaran dan Pembatalan Pengguna (*User Registration and Deregistration*)

Peranan: Pentadbir Sistem ICT / Pengguna

Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi:

(i) Akaun yang diperuntukkan oleh LLM sahaja boleh digunakan;
(ii) Akaun pengguna mestilah unik;
(iii) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada LLM terlebih dahulu;
(iv) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
(v) Pemilikan akaun bukanlah hak mutlak pengguna dan boleh ditarik balik jika penggunaannya melanggar peraturan LLM; dan
(vi) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan LLM dan didokumentasikan.

A.5.2.2 Peruntukan Akses Pengguna (*User Access Provisioning*)

Peranan: Pentadbir Sistem ICT / Pengarah Bahagian

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 :

(i) Mendapatkan kebenaran daripada pemilik sistem atau perkhidmatan ICT;
(ii) Menentusahkan tahap akses yang diberikan adalah wajar dan selaras dengan keperluan tugas;
(iii) Memastikan hak akses tidak diaktifkan sebelum prosedur kebenaran dilengkapkan;
(iv) Mengekalkan rekod berpusat untuk hak akses yang diberikan kepada ID Pengguna;
(v) Menyesuaikan hak akses pengguna yang menukar peranan atau pekerjaan dan segera menyekat atau menghapuskan hak akses pengguna yang telah meninggalkan organisasi; dan
(vi) Mengkaji semula secara berkala hak akses tersebut.

A.5.2.3 Pengurusan Hak Akses Istimewa (*Management of Privileged Access Rights*)

Peranan: Pentadbir Sistem ICT

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.

A.5.2.4 Pengurusan Maklumat Pengesahan Rahsia Pengguna (*Management of Secret Authentication Information of Users*)

Peranan: Pentadbir Sistem ICT

Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.

A.5.2.5 Kajian Semula Hak Akses Pengguna (*Review of User Access Rights*)

Peranan: Pentadbir Sistem ICT

Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan.

Pentadbir Sistem ICT perlu menyemak hak akses pengguna secara berkala ke atas sistem aplikasi untuk memastikan capaian hanya dibuat oleh pengguna yang sah.

A.5.2.6 Pembatalan atau Pelarasan Hak Akses (*Removal or Adjustment of Access Rights*)

Peranan: Pentadbir Sistem ICT

Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikemaskini mengikut keperluan semasa.

A.5.3 Tanggungjawab Pengguna (*User Responsibilities*)

Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.

A.5.3.1 Pengurusan Maklumat Pengesahan Rahsia Pengguna (*Management of Secret Authentication Information of Users*)

Peranan: Pengguna, Pentadbir Sistem ICT / Pengarah Teknologi Maklumat

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

(i) Membaca, memahami dan mematuhi Polisi Keselamatan Siber (PKS) Lembaga Lebuhraya Malaysia;
(ii) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;
(iii) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat LLM;
(iv) Melaksanakan langkah-langkah perlindungan seperti yang berikut:
  (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
  (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
  (c) Menentukan maklumat sedia untuk digunakan;
  (d) Menjaga kerahsiaan kata laluan;
  (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
  (f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
  (g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

(v) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan

(vi) Menghadiri program-program kesedaran mengenai keselamatan siber.

A.5.3.2 Penggunaan Maklumat Pengesahan Rahsia (*Use of Secret Authentication Information*)

Peranan: Pentadbir Sistem ICT / Pengguna

Pengguna perlu mengikut amalan keselamatan yang baik dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.

A.5.4 Kawalan Akses Sistem dan Aplikasi (*System and Application Access Control*)

Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.

A.5.4.1 Sekatan Akses Maklumat (*Information Access Restriction*)

Peranan: Pentadbir Sistem ICT / Pengguna

Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.

A.5.4.2 Prosedur Log Masuk yang Selamat (*Secure Log-On Procedure*)

Peranan: Pentadbir Sistem ICT

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 yang berikut:

(i) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan LLM;

(ii) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem;

(iii) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin;

(iv) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna;

(v) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti;

(vi) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.

A.5.4.3 Sistem Pengurusan Kata Laluan (*Password Management System*)

Peranan: Pentadbir Sistem ICT / Pengguna

Sistem pengurusan kata laluan hendaklah interaktif dan mengambil kira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh LLM seperti yang berikut:

(i) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

(ii) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

(iii) Panjang kata laluan mestilah sekurang-kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (*alphanumeric*) **KECUALI** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad.

(iv) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun;

(v) Kata laluan paparan kunci (*lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

(vi) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain;

(vii) Kuatkuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan;

(viii) Kata laluan mestilah ditukar setiap enam bulan sekali bagi menjamin keselamatan ; dan

(ix) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.

A.5.4.4 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa (*Use of Privileged Utility Programs*)

Peranan: Pengarah Teknologi Maklumat / Pentadbir Sistem ICT

Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.

A.5.4.5 Kawalan Akses Kepada Kod Sumber Program (*Access Control to Program Source Code*)

Peranan: Pengarah Projek / Pengurus Projek / Pentadbir Sistem ICT

Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan

(ii) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik LLM.

BIDANG A.6

KRIPTOGRAFI (*CRYPTOGRAPHY*)

A.6.1 Kawalan Kriptografi

(*Cryptography Controls*)

A.6.1.1 Polisi Penggunaan Kawalan Kriptografi

(*Policy on The Use of Cryptographic Control*)

A.6.1.2 Pengurusan Kunci Awam

(*Public Key Management*)

A.6.1.3 *Data Masking*

A.6.1 KAWALAN KRIPTOGRAFI (*CRYPTOGRAPHY CONTROLS*)

Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan dan/atau keutuhan maklumat.

A.6.1.1 Polisi Penggunaan Kawalan Kriptografi (*Policy on The Use of Cryptographic Control*)

Peranan: Pengarah Projek

Kriptografi merangkumi kaedah-kaedah seperti yang berikut:

(i) **Enkripsi**

Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*).

(ii) **Tandatangan Digital**

Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan.

A.6.1.2 Pengurusan Kunci Awam (*Public Key Management*)

Peranan: Pentadbir Sistem ICT

Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam/*Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

A.6.1.3 *Data Masking*

Peranan: Pentadbir Sistem Aplikasi, pihak ketiga

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 data peribadi (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.

BIDANG A.7
KESELAMATAN FIZIKAL DAN PERSEKITARAN
(*PHYSICAL AND ENVIRONMENTAL SECURITY*)

A.7.1 Kawasan Selamat

(*Secure Areas*)

A.7.1.1 Perimeter Keselamatan Fizikal

(*Physical Security Parameter*)

A.7.1.2 Kawalan Kemasukan Fizikal

(*Physical Entry Controls*)

A.7.1.3 Keselamatan Pejabat, Bilik dan Kemudahan

(*Securing Offices, Rooms and Facilities*)

A.7.1.4 Perlindungan Daripada Ancaman Luar Dan Persekitaran

(*Protecting Against External and Environmental Threats*)

A.7.1.5 Bekerja di Kawasan Selamat

(*Working in Secure Areas*)

A.7.1.6 Kawasan Penyerahan dan Pemunggahan

(*Delivery and Loading Areas*)

A.7.2 Peralatan ICT

(*ICT Equipment*)

A.7.2.1 Penempatan dan Perlindungan Peralatan ICT

(*Equipment Sitting and Protection*)

A.7.2.2 Utiliti Sokongan

(*Supporting Utilities*)

A.7.2.3 Keselamatan Kabel

(*Cabling Security*)

A.7.2.4 Penyenggaraaan Peralatan

(*Equipment Maintenance*)

A.7.2.5 Pengalihan Aset

(*Removal of Assets*)

A.7.2.6 Keselamatan Peralatan dan Aset di Luar Premis

(*Security of Equipment Off-Premises*)

A.7.2.7 Pelupusan yang Selamat atau Penggunaan Semula Peralatan

(*Secure Disposal or Re-Use of Equipment*)

A.7.2.8 Peralatan Pengguna Tanpa Kawalan

(*Unattended User Equipment*)

A.7.2.9 Dasar Meja Kosong dan Skrin Kosong

(*Clear Desk dan Clear Screen Policy*)

A.7.2.10 *Physical Security Monitoring*

A.7.1 KAWASAN SELAMAT (*SECURE AREAS*)

Objektif: Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat LLM.

A.7.1.1 Perimeter Keselamatan Fizikal (*Physical Security Parameter*)

Peranan: Pejabat Ketua Pegawai Keselamatan Kerajaan, Pegawai Keselamatan Pejabat

Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan Aset ICT LLM. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

(i) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;

(ii) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;

(iii) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan fasiliti pejabat;

(iv) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia;

(v) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad;

(vi) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan

(vii) Memasang alat penggera atau kamera keselamatan

A.7.1.2 Kawalan Kemasukan Fizikal (*Physical Entry Controls*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis LLM. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Setiap pegawai dan kakitangan LLM hendaklah menggunakan sistem biometrik yang digunakan untuk mengawal akses keluar dan masuk di kasawan pejabat;

(ii) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan;

(iii) Kehilangan pas hendaklah dilaporkan segera kepada Pihak Bertanggungjawab.

A.7.1.3 Keselamatan Pejabat, Bilik dan Kemudahan (*Securing Offices, Rooms and Facilities*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Keselamatan fizikal untuk pejabat, bilik dan fasiliti pejabat hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Kawasan tempat bekerja, bilik mesyuarat, bilik perbincangan, bilik fail, bilik cetakan, dan pusat data perlu dihadkan daripada diakses tanpa kebenaran;

(ii) Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan

(iii) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.

A.7.1.4 Perlindungan Daripada Ancaman Luar Dan Persekitaran (*Protecting Against External and Environmental Threats*).

Peranan: Pentadbir Pusat Data

Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. LLM perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.

A.7.1.5 Bekerja di Kawasan Selamat (*Working in Secure Area*)

Peranan: Pentadbir Pusat Data

Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga LLM yang tertentu sahaja. lni dilakukan untuk melindungi aset ICT yang terdapat dalam premis LLM termasuklah Pusat Data.

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut:

(i) 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;

(ii) Akses adalah terhad kepada warga LLM yang telah diberi kuasa sahaja dan dipantau pada setiap masa;

(iii) Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai;

(iv) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;

(v) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;

(vi) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;

(vii) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam;

(viii) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan;

(ix) Memperkukuh dinding dan siling; dan

(x) Mengehadkan jalan keluar masuk.

A.7.1.6 Kawasan Penyerahan dan Pemunggahan (*Delivery and Loading Areas*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM.

Titik kemasukan *access point* seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan.

LLM hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.

A.7.2 PERALATAN ICT (*ICT EQUIPMENT*)

Objektif: Melindungi peralatan ICT LLM daripada kehilangan, kerosakan, kecurian dan disalahgunakan.

A.7.2.1 Penempatan dan Perlindungan Peralatan ICT (*Equipment Sitting and Protection*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

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:

(i) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

(ii) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

(iii) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

(iv) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;

(v) 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;

(vi) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna;

(vii) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;

(viii) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set);

(ix) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan.

(x) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci;

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

(xii) Peralatan ICT yang hendak dibawa ke luar premis LLM, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;

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

(xiv) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

(xv) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

(xvi) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih;

(xvii) 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;

(xviii) Konfigurasi Alamat IP juga tidak dibenarkan diubah daripada Alamat IP yang asal;

(xix) Pengguna dilarang sama sekali mengubah *password administrator* yang telah ditetapkan oleh pihak ICT; dan

(xx) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan LLM sahaja.

A.7.2.2 Utiliti Sokongan (*Supporting Utilities*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara secara berkala.

A.7.2.3 Keselamatan Kabel (*Cabling Security*)

Peranan: Pentadbir Sistem ICT

Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan.

Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:

(i) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;

(ii) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;

(iii) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

(iv) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.

7.2.4 Penyelenggaraan Peralatan (*Equipment Maintenance*)

Peranan: Pegawai Aset, Pentadbir Sistem ICT

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:

(i) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;

(ii) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;

(iii) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

(iv) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan

(v) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikul jadual yang ditetapkan atau atas keperluan.

A.7.2.5 Pengalihan Aset (*Removal of Assets*)

Peranan: Pengguna, Pegawai 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:

(i) Peralatan ICT gunasama yang hendak dibawa keluar dari premis LLM untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Pengarah LLM atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan

(ii) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.

A.7.2.6 Keselamatan Peralatan dan Aset di Luar Premis (*Security of Equipment Off-Premises*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis LLM. Peralatan yang dibawa keluar dari premis LLM adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Peralatan perlu dilindungi dan dikawal sepanjang masa;

(ii) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan

(iii) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan

A.7.2.7 Pelupusan yang Selamat atau Penggunaan Semula Peralatan (*Secure Disposal or Re-Use of Equipment*)

Peranan: Pegawai Aset, Pentadbir Sistem ICT dan warga LLM

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 LLM dan ditempatkan di LLM.

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 LLM. Langkah-langkah seperti yang berikut hendaklah diambil:

(i) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat;

(ii) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

(iii) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

(iv) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;

(v) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti yang berikut:

(a) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.
(b) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman
(c) CPU seperti RAM, *Hardisk*, *Motherboard* dan sebagainya.
(d) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di LLM.
(e) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan
(f) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab LLM.

(vi) 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.

(vii) 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;

(viii) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa;

(ix) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan

(x) Pegawai asset aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset.

A.7.2.8 Peralatan Pengguna Tanpa Kawalan (*Unattended User Equipment*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:

(i) Tamatkan sesi aktif apabila selesai tugas;

(ii) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan

(iii) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.

A.7.2.9 Dasar Meja Kosong dan Skrin Kosong (*Policy Clear Desk dan Clear Screen*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM.

Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Clear Desk bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuklah seperti yang berikut:

(i) Menggunakan kemudahan password *screensaver* atau *logout* apabila meninggalkan komputer;

(ii) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;

(iii) Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin *faksimile* dan mesin fotostat.

(iv) E-mel masuk dan keluar hendaklah dikawal; dan

(v) Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.

A.7.2.10 *Physical Security Monitoring*

Peranan: Pegawai Keselamatan Jabatan LLM

Kawalan pemantauan keselamatan fizikal perlu dipantau secara berterusan bagi mengelakkan akses tanpa kebenaran daripada pihak yang tidak bertanggungjawab.

BIDANG A.8

KESELAMATAN OPERASI (*OPERATIONS SECURITY*)

A.8.1 Prosedur dan Tanggungjawab Operasi

(*Operational Procedures Responsibilities*)

A.8.1.1 Pengendalian Prosedur Operasi

(*Handling of Operational Procedures*)

A.8.1.2 Pengurusan Perubahan

(*Change Management*)

A.8.1.3 Pengurusan Kapasiti

(*Capacity Management*)

A.8.1.4 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi

(*Segregation of Development, Testing and Operational Environment*)

A.8.2 Perlindungan daripada Perisian Hasad

(*Controls Against Malware*)

A.8.2.1 Kawalan Daripada *Malware*

(*Controls Against Malware*)

A.8.3 Sandaran

(*Backup*)

A.8.3.1 Sandaran Maklumat

(*Information Backup*)

A.8.4 Log dan Pemantauan

(*Logging and Monitoring*)

A.8.4.1 Log Kejadian dan Perlindungan Maklumat Log

(*Event Log and Protection of Log Information*)

A.8.4.2 Perlindungan Maklumat Log

(*Protection of Log Information*)

A.8.4.3 Log Pentadbir dan Pengendali

(*Administrator & Operator Log*)

A.8.4.4 Penyeragaman Masa

(*Time Synchronizations*)

A.8.5 Kawalan Perisian Yang Beroperasi

(*Control Of Operational Software*)

A.8.5.1 Pemasangan Perisian Pada Sistem Yang Beroperasi

(*Installation of Software on Operational Systems*)

A.8.6 Pengurusan Kerentanan Teknikal

(*Technical Vulnerability Management)*

A.8.6.1 Pengurusan Kerentanan Teknikal

(*Management of Technical Vulnerabilities*)

A.8.6.2 Sekatan Ke Atas Pemasangan Perisian

(*Restriction on Software Installation*)

A.8.7 Pertimbangan Tentang Audit Sistem

(*Systems Audit Considerations***)**

A.8.7.1 Kawalan Audit Sistem Maklumat

(*Information Systems Audit Controls*)

A.8.7.2 *Information Security For Use Of Cloud Services*

A.8.7.3 *Threat Intelligence*

A.8.7.4 *Configuration Management*

A.8.7.5 *Monitoring Activities*

A.8.7.6 *Web Filtering*

A.8.7.7 *Information Deletion*

A.8.1 PROSEDUR DAN TANGGUNGJAWAB OPERASI (*OPERATIONAL PROCEDURES AND RESPONSIBILITIES*)

Objektif: Memastikan pengurusan operasi pemprosesan maklumat dilaksanakan dengan cekap dan selamat.

A.8.1.1 Pengendalian Prosedur Operasi (*Handling of Operational Procedures*)

Peranan: Pengarah Bahagian dan Pentadbir Sistem ICT

Semua prosedur pengurusan operasi hendaklah dikenal pasti, didokumenkan, disimpan dan dihadkan capaian berdasarkan keperluan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Semua prosedur operasi hendaklah didokumenkan dengan jelas, teratur, dikemaskinikan dan sedia digunapakai oleh pengguna;

(ii) Setiap perubahan kepada prosedur operasi mestilah dikawal;

(iii) Tugas dan tanggungjawab fungsi perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset ICT LLM; dan

(iv) Kemudahan ICT untuk kerja-kerja pembangunan, pengujian dan operasi perlu diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.

A.8.1.2 Pengurusan Perubahan (*Change Management*)

Peranan: Pemilik Sistem, Pentadbir Sistem ICT

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:

(i) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;

(ii) 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 secara langsung dengan aset ICT berkenaan;

(iii) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan

(iv) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.

A.8.1.3 Pengurusan Kapasiti (*Capacity Management*)

Peranan: Pengarah Teknologi Maklumat, Pentadbir Sistem ICT

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:

(i) 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

(ii) 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.

A.8.1.4 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi (*Segregation of Development, Testing and Operational Environment*)

Peranan: Pengarah Teknologi Maklumat, Pentadbir Sistem ICT

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan daripada perkakasan yang digunakan dalam pengoperasian sebenar (*production environment*).

(ii) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan

(iii) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

A.8.2 PERLINDUNGAN DARIPADA MALWARE (*PROTECTION FROM MALWARE*)

Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.

A.8.2.1 Kawalan Daripada Perisian Hasad (*Controls Against Malware*)

Peranan: ICTSO, Pentadbir Sistem ICT, Pengguna

Aset ICT perlu dilindungi supaya tidak terdedah kepada kerosakan yang disebabkan oleh kod hasad seperti *virus, worm, trojan* dan seumpamanya.

Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut.

Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut:

(i) Memasang sistem keselamatan untuk mengesan perisian hasad atau *malware* seperti *antivirus, Intrusion Detection System* (IDS) atau *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;

(ii) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;

(iii) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;

(iv) Mengemaskini *antivirus* dengan *signature/pattern antivirus* yang terkini;

(v) Mengemaskini *patches* sistem pengoperasian pada peralatan ICT;

(vi) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

(vii) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

(viii) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan;

(ix) Memberi amaran mengenai ancaman seperti serangan virus terhadap keselamatan aset ICT LLM;

(x) Melaksanakan Program Kesedaran Pengguna yang bersesuaian; dan

(xi) Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

A.8.3 SANDARAN (*BACKUP*)

Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.

A.8.3.1 Sandaran Maklumat (*Information Backup*)

Peranan: Pentadbir Sistem ICT

Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *offsite*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau sebelum melaksanakan sebarang kemaskini/ penaiktarafan yang kritikal;

(ii) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi;

(iii) Menguji sistem sandaran sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan

(iv) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara **harian**, **mingguan**, **bulanan** atau **tahunan**.

A.8.4 LOG DAN PEMANTAUAN (*LOGGING AND MONITORING*)

Objektif: Merekodkan peristiwa dan menghasilkan bukti.

A.8.4.1 Log Kejadian dan Perlindungan Maklumat Log (*Event Log and Protection of Log Information*)

Peranan: ICTSO, Pentadbir Sistem ICT

Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti- aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.

Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Fail log sistem pengoperasian;
(ii) Fail log servis (contoh: web, e-mel);
(iii) Fail log aplikasi (*audit trail*); dan
(iv) Fail log rangkaian (contoh: *switch, firewall*, IPS).

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

(i) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
(ii) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera;
(iii) Sebarang aktiviti tidak sah seperti kecurian maklumat dan pencerobohan hendaklah dilaporkan kepada CERT LLM.

A.8.4.2 Perlindungan Maklumat Log (*Protection of Log Information*)

Peranan: Pentadbir Sistem ICT

Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.

A.8.4.3 Log Pentadbir dan Pengendali (*Administrator & Operator Log*)

Peranan: Pentadbir Sistem ICT dan CERT LLM

Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap.

(i) Memantau penggunaan kemudahan memproses maklumat secara berkala;

(ii) Aktiviti pentadbiran dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu;

(iii) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;

(iv) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan

(v) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada pasukan CERT LLM.

A.8.4.4 Penyeragaman Masa (*Time Synchronizations*)

Peranan: Pentadbir Sistem ICT

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 LLM atau domain keselamatan perlu diseragamkan dengan sumber waktu yang ditetapkan oleh National Metrology Institute of Malaysia (**NMIM**).

A.8.5 KAWALAN PERISIAN YANG BEROPERASI (*CONTROL OF OPERATIONAL SOFTWARE*)

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

A.8.5.1 Pemasangan Perisian Pada Sistem Yang Beroperasi (*Installation of Software on Operational Systems*)

Peranan: Pengarah Bahagian dan Pentadbir Sistem ICT

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 berikut:

(i) Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;

(ii) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan

(iii) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

A.8.6 Pengurusan Kerentanan Teknikal (*Technical Vulnerability Management*)

Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.

A.8.6.1 Pengurusan Kerentanan Teknikal (*Management of Technical Vulnerabilities*)

Peranan: Pentadbir Sistem ICT dan CERT LLM

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 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:

(i) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;

(ii) Menganalisis tahap risiko kerentanan; dan

(iii) Mengambil tindakan pengolahan dan kawalan risiko.

A.8.6.2 Sekatan Ke Atas Pemasangan Perisian (*Restriction on Software Installation*)

Peranan: Pentadbir Sistem ICT, warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital LLM;

(ii) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan

(iii) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.

A.8.7 PERTIMBANGAN TENTANG AUDIT SISTEM (*SYSTEMS AUDIT CONSIDERATIONS*)

Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.

A.8.7.1 Kawalan Audit Sistem Maklumat (Information Systems Audit Controls)

Peranan: ICTSO, Pentadbir Sistem ICT

Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas operasi harian.

A.8.7.2 *Information Security For Use Of Cloud Services*

Peranan: CIO dan ICTSO

Pelaksanaan pengkomputeran awan perlu mematuhi aspek keselamatan kerana menyerahkan ketersediaan keselamatan data aplikasi dan infrastruktur ICT kepada pihak ketiga. LLM perlulah memastikan perkhidmatan ini dilindungi dengan kehendak undang-undang dan hak kontraktual. Antara risiko kebergantungan kepada pihak ketiga yang boleh menyebabkan risiko keselamatan yang tidak diketahui dan disedari adalah seperti kebergantungan pengurusan rantaian bekalan (*supply chain management*) *multitenancy* kepada sumber ICT yang telah dibayar, ancaman daripada sumber dalaman pembekal, *vendor lock in* dan privasi.

A.8.7.3 *Threat Intelligence*

Peranan: Pentadbir Sistem ICT

Operasi rangkaian dan infrastruktur LLM dipantau menggunakan perkakasan dan perisian tertentu. Rekod aktiviti dan log dikumpulkan dan dianalisa bagi mengenalpasti ancaman serangan siber bagi membolehkan tindakan mitigasi diambil secara tepat dan berkesan.

Analisa yang dikenalpasti dikategorikan kepada tiga jenis maklumat ancaman iaitu kaedah serangan, metodologi serangan dan perincian maklumat penyerang.

A.8.7.4 *Configuration Management*

Peranan: Pentadbir Sistem ICT

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.

A.8.7.5 *Monitoring Activities*

Peranan: Pentadbir Sistem ICT

Untuk mengesan lebih awal perbuatan yang mencurigakan bagi mengelakkan berlakunya insiden dengan pemantauan ke atas tiga (3) perkara asas iaitu jalur lebar (*bandwidth),* rangkaian dan sistem aplikasi yang mencurigakan.

A.8.7.6 *Web Filtering*

Peranan: Pentadbir Sistem ICT

Untuk melindungi sistem daripada terjejas oleh perisian berbahaya dan untuk menghalang akses kepada web yang tidak dibenarkan. LLM 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.

LLM perlu mengesan dan menyekat alamat IP dan domain laman web yang diragui untuk mengawal akses kepada kandungan yang mungkin tidak sesuai atau berpotensi membahayakan pengguna terutamanya dalam persekitaran organisasi kerajaan.

A.8.7.7 *Information Deletion*

Peranan: Pentadbir Sistem ICT

LLM 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*).

BIDANG A.9

KESELAMATAN KOMUNIKASI (*COMMUNICATIONS SECURITY*)

A.9.1 Pengurusan Keselamatan Rangkaian

(*Network Security Management*)

A.9.1.1 Kawalan Rangkaian

(*Network Controls*)

A.9.1.2 Keselamatan Perkhidmatan Rangkaian

(*Security of Network Services*)

A.9.1.3 Pengasingan Rangkaian

(*Segregation in Networks*)

A.9.2 Pemindahan Data dan Maklumat

(*Information Transfer*)

A.9.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat

(*Information Transfer Policies and Procedures*)

A.9.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat

(*Agreements on Information Transfer*)

A.9.2.3 Pengurusan Pesanan Elektronik

(*Electronic Messaging Management*)

A.9.2.4 Perjanjian Kerahsiaan atau Ketakdedahan

(*Confidentiality Or Non-Disclosure Agreement*)

A.9.2.5 *Data Leakage Prevention*

A.9.1 PENGURUSAN KESELAMATAN RANGKAIAN (*NETWORK SECURITY MANAGEMANT*)

Objektif: Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

A.9.1.1 Kawalan Rangkaian (Network Controls)

Peranan: ICTSO / Pengarah Teknologi Maklumat / Pentadbir Sistem ICT / Pentadbir Rangkaian

Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

(i) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan;

(ii) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko seperti banjir, gegaran dan habuk;

(iii) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;

(iv) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check (*FAC) semasa pemasangan dan konfigurasi;

(v) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian;

(vi) Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan LLM;

(vii) Semua perisian *sniffer* atau *Network Analyzer* adalah dilarang dipasang pada komputer pengguna **KECUALI** mendapat kebenaran daripada Pegawai Keselamatan Teknologi Maklumat (ICTSO).

(viii) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat LLM;

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

(x) Sebarang aktiviti penyambungan rangkaian yang bukan di bawah kawalan BTM LLM adalah tidak dibenarkan;

(xi) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di LLM sahaja dan penggunaan modem adalah dilarang sama sekali;

(xii) Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya;

(xiii) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurances* (SLA) yang telah ditetapkan;

(xiv) Menempatkan atau memasang antara muka (*interface*) yang bersesuaian antara rangkaian LLM, rangkaian agensi lain dan rangkaian awam;

(xv) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;

(xvi) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja;

(xvii) Mengawal capaian fizikal dan logikal ke atas kemudahan *port* diagnostic dan konfigurasi jarak jauh;

(xviii) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan LLM; dan

(xix) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan LLM

A.9.1.2 Keselamatan Perkhidmatan Rangkaian (*Security of Network Services*)

Pengurusan bagi semua perkhidmatan rangkaian (*inhouse* atau *outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan rangkaian.

Peranan: ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT dan Pembekal

A.9.1.3 Pengasingan Rangkaian (*Segregation in Networks*)

Peranan: ICTSO, Pengarah Bahagian dan Pentadbir Sistem ICT

Pengasingan perkhidmatan rangkaian bertujuan meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan.

Perkara–perkara yang perlu dipatuhi adalah:

(i) Melaksanakan konfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan;

(ii) Menyediakan rangkaian terasing (*isolated network*) untuk orang luar atau pelawat yang hadir ke pejabat LLM dan memerlukan capaian Internet. Rangkaian ini hendaklah tidak dibenarkan mengakses rangkaian dalaman LLM dan perlu dipantau dari semasa ke semasa.

(iii) Mengemaskini hak capaian pengguna dari semasa ke semasa mengikut keperluan.

A.9.2 PEMINDAHAN DATA DAN MAKLUMAT (*INFORMATION TRANSFER*)

Objektif: Memastikan keselamatan perpindahan/pertukaran data maklumat dan perisian antara LLM dan pihak luar terjamin.

A.9.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat (*Information Transfer Policies and Procedures*)

Peranan: Pengguna, warga LLM dan pembekal

Prosedur ini bertujuan untuk mengendali, menyimpan, memindah serta melindungi maklumat daripada didedah tanpa kebenaran atau salah guna serta memastikan keselamatan pemindahan maklumat dengan entiti luar terjamin. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi;

(ii) Terma pemindahan data, maklumat dan perisian antara LLM dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;

(iii) Media yang mengandungi maklumat perlu dilindungi;

(iv) Sebarang pemindahan maklumat di antara LLM dan agensi lain mestilah dikawal; dan

(v) Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.

A.9.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat (*Agreements on Information Transfer*)

Peranan: CIO dan Pengarah Bahagian

LLM perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara LLM dengan pihak luar. Perkara yang perlu dipertimbangkan ialah:

(i) Penghantaran dan penerimaan maklumat LLM hendaklah dalam keadaan terkawal;

(ii) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat LLM;

(iii) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan

(iv) LLM hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan mencegah ketirisan data.

A.9.2.3 Pengurusan Pesanan Elektronik (*Electronic Messaging Management*)

Peranan: Warga LLM

Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti **LAMPIRAN A**:

(i) Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003;

(ii) Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 - Pematuhan Tatacara Penggunaan E-mel dan Internet; dan

(iii) Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa.

A.9.2.4 Perjanjian Kerahsiaan atau Ketakdedahan (*Confidentiality Or Non-Disclosure Agreement*)

Peranan: ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT, Pengguna dan Pembekal

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 dan mematuhi semua keperluan keselamatan maklumat.

A.9.2.5 *Data Leakage Prevention*

Peranan: ICTSO, CIO, Pengarah Bahagian, Pentadbir Sistem ICT, Pengguna dan Pembekal

LLM 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.

BIDANG A.10

PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM (*SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE*)

A.10.1 Keperluan Keselamatan Sistem Maklumat

(*Security Requirements of Information Systems*)

A.10.1.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat

(*Information Security Requirements Analysis and Spesifications*)

A.10.1.2 Melindungi Perkhidmatan Aplikasi Dalam Rangkaian Awam

(*Securing Application Services on Public Networks*)

A.10.1.3 Melindungi Transaksi Perkhidmatan Aplikasi

(*Protecting Application Services Transaction*)

A.10.2 Keselamatan Dalam Proses Pembangunan Dan Sokongan

(*Security in Development and Support Services*)

A.10.2.1 Polisi Keselamatan Dalam Pembangunan Sistem

(*Security Policy In System Development*)

A.10.2.2 Prosedur Kawalan Perubahan Sistem

(*System Change Control Procedures*)

A.10.2.3 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi

(*Technical Review Of Applications After Operating Platform Changes*)

A.10.2.4 Sekatan Ke atas Perubahan Dalam Pakej Perisian

(*Restrictions on Changes to Software Packages*)

A.10.2.5 Prinsip Kejuruteraan Sistem Yang Selamat

(*Secure System Engineering Principles*)

A.10.2.6 Persekitaran Pembangunan Sistem Yang Selamat

(*Secure Development Environment*)

A.10.2.7 Pembangunan Sistem Secara Khidmat Luaran

(Outsourced Software Development)

A.10.2.8 Pengujian Keselamatan Sistem

(System Security Testing)

A.10.2.9 Pengujian Penerimaan Sistem

(System Acceptance Testing)

10.2.10 *Secure coding*

A.10.3 Data Ujian

(*Test Data*)

A.10.3.1 Perlindungan Data Ujian

(*Protection of Test Data*)

A.10.1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT (*SECURITY REQUIREMENTS OF INFORMATION SYSTEMS*)

Objektif: Memastikan keperluan keselamatan diambil kira dalam setiap fasa kitar hayat pembangunan sistem maklumat.

A.10.1.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat (*Information Security Requirements Analysis and Spesifications*)

Peranan: Pentadbir Sistem ICT, Pembekal

Pembangunan sistem baharu atau penambahbaikan sistem sedia ada hendaklah mematuhi perkara-perkara berikut:

(i) Semua sistem yang dibangunkan sama ada secara dalaman atau khidmat luaran hendaklah dikaji supaya mengikut keperluan 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);

(ii) 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;

(iii) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber LLM;

(iv) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan;

(v) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang ditetapkan; dan

(vi) Ujian keselamatan hendaklah dilakukan di setiap peringkat pembangunan sistem bagi memastikan integriti data.

A.10.1.2 Melindungi Perkhidmatan Aplikasi Dalam Rangkaian Awam (*Securing Application Services on Public Networks*)

Peranan: Pengarah Teknologi Maklumat, Pentadbir Sistem ICT, Pembekal

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:

(i) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;

(ii) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;

(iii) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan MFA (*Multi Factor Authentication*);

(iv) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;

(v) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan

(vi) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.

A.10.1.3 Melindungi Transaksi Perkhidmatan Aplikasi (*Protecting Application Services Transaction*)

Peranan: Pengarah Teknologi Maklumat, Pentadbir Sistem ICT

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:

(i) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;

(ii) Memastikan semua aspek transaksi dipatuhi:
   (a) Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan;
   (b) Mengekalkan kerahsiaan maklumat;
   (c) Mengekalkan privasi pihak yang terlibat; dan
   (d) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi.

(iii) Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.

A.10.2 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN (*SECURITY IN DEVELOPMENT AND SUPPORT SERVICES*)

Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

A.10.2.1 Polisi Keselamatan Dalam Pembangunan Sistem (*Security Policy In System Development*)

Peranan: ICTSO, Pengarah Teknologi Maklumat & Pentadbir Sistem ICT

Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Keselamatan persekitaran pembangunan;
(ii) Keselamatan pangkalan data;
(iii) Keperluan keselamatan dalam fasa reka bentuk;
(iv) Keperluan pengetahuan ke atas keselamatan aplikasi;
(v) Keselamatan dalam kawalan versi; dan
(vi) Bagi pembangunan melalui khidmat sumber luaran (*outsource*), pembekal yang dilantik hendaklah berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.

A.10.2.2 Prosedur Kawalan Perubahan Sistem (*System Change Control Procedures*)

Peranan: Pengarah Bahagian dan Pentadbir Sistem ICT

Prosedur kawalan perubahan sistem hendaklah diwujudkan bagi mengawal sebarang perubahan ke atas sistem maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, didokumenkan dan disahkan sebelum diguna pakai;

(ii) Setiap aplikasi perlu dikaji semula dan diuji apabila terdapat perubahan/naiktaraf sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;

(iii) Kawalan perlu dibuat terhadap sebarang perubahan ke atas sistem aplikasi atau pakej perisian bagi memastikan perisian terhad mengikut keperluan sahaja; dan

(iv) Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.

A.10.2.3 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi (*Technical Review Of Applications After Operating Platform Changes*)

Peranan: Pentadbir Sistem ICT

Sebarang cadangan perubahan platform hendaklah berasaskan kepada kajian teknikal bagi memastikan pengoperasian sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Memastikan sistem aplikasi dan integriti data disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilakukan;

(ii) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan

(iii) Sebarang perubahan hendaklah selari dengan Pelan Kesinambungan Perkhidmatan LLM.

A.10.2.4 Sekatan Ke atas Perubahan Dalam Pakej Perisian (*Restrictions on Changes to Software Packages*)

Peranan: Pentadbir Sistem ICT, Pengarah Bahagian

Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.

A.10.2.5 Prinsip Kejuruteraan Sistem Yang Selamat (*Secure System Engineering Principles*)

Peranan: Pentadbir Sistem ICT, Pengarah Bahagian

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. Semua peringkat pembangunan sistem hendaklah mengambil kira prinsip kejuruteraan sistem berikut:

(i) Asas Keselamatan (*Security Foundation*)

Merujuk kepada PKS LLM dan pekeliling semasa yang berkuat kuasa dalam reka bentuk sesuatu sistem seperti Panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA) dan *Enterprise Architecture* Sektor Awam (EA).

(ii) Berasaskan Risiko (*Risk Based*)

Mengurangkan risiko ke tahap boleh terima.

(iii) Mudah Diguna (*Ease of Use*)

Mempunyai ciri-ciri *open standard* untuk *portability* dan *interoperability*.

(iv) Meningkatkan Daya Tahan (*Increase Resilience*)

Memastikan tiada sebarang kelemahan melalui pelaksanaan keselamatan (*layered security*).

(v) Mengurang Kelemahan (*Reduce Vulnerabilities*)

Meminimumkan kelemahan disebabkan reka bentuk yang kompleks supaya penyenggaraan sistem mudah dilaksanakan.

(vi) Mengambil kira Keperluan Rangkaian dalam Reka Bentuk Sistem (*Design with Network in Mind*)

Pelaksanaan keselamatan hendaklah mengambil kira capaian sistem dari dalam dan luar premis.

A.10.2.6 Persekitaran Pembangunan Sistem Yang Selamat (*Secure Development Environment*)

Peranan: Pentadbir Sistem ICT

Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.

Adalah perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:

(i) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;
(ii) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;
(iii) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;
(iv) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;
(v) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan
(vi) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.

A.10.2.7 Pembangunan Sistem Secara Khidmat Luaran (*Outsourced Development*)

Peranan: Pentadbir Sistem ICT, Pengarah Bahagian, ICTSO

Pembangunan sistem secara khidmat sumber luaran perlu dikawal selia dan dipantau. *Intellectual Property Rights* (IPR) dan kod sumber (*source code*) hendaklah menjadi hak milik Kerajaan.

Semasa fasa pembangunan sistem oleh pihak tersebut, kod sumber (*source code*) yang dibangunkan perlu diakses dan disemak oleh LLM mengikut pekeliling semasa yang berkuat kuasa seperti Panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA) dan *Enterprise Architecture* Sektor Awam (EA).

LLM hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara outsource oleh pihak luar. Kod sumber (*source code*) adalah menjadi **HAK MILIK LLM**. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Perkiraan perlesenan, kod sumber ialah **HAK MILIK LLM** dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*;

(ii) 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";

(iii) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik;

(iv) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;

(v) Mengguna pakai prinsip dan tatacara *escrow*; dan

(vi) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.

A.10.2.8 Pengujian Keselamatan Sistem (*System Security Testing*)

Peranan: Pentadbir Sistem ICT

Ujian keselamatan sistem hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (*input*), peringkat pemprosesan data (*process*) dan peringkat penjanaan laporan (*output*). Perkara–perkara yang perlu dipatuhi oleh pentadbir sistem adalah:

(i) Merancang dan melaksanakan penilaian risiko mengikut keperluan bagi mengenal pasti dan melaksana kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi;

(ii) Merancang dan melaksana ujian keselamatan yang bersesuaian mengikut fasa di dalam kitar hayat pembangunan sistem (*Software Development Life Cycle* atau SDLC), Panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA) dan *Enterprise Architecture* Sektor Awam (EA) bagi mengenal pasti kelemahan sistem;

(iii) Membuat semakan pengesahan sistem aplikasi untuk mengenal pasti sebarang pencemaran maklumat sama ada disebabkan oleh kesilapan atau disengajakan;

(iv) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;

(v) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan

(vi) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.

A.10.2.9 Pengujian Penerimaan Sistem (*System Acceptance Testing*)

Peranan: Pengguna, Pentadbir Sistem ICT, ICTSO

Program Pengujian Penerimaan Sistem (Ujian Penerimaan Pengguna dan Ujian Penerimaan Akhir) hendaklah dilaksanakan berdasarkan kriteria yang telah ditetapkan sebelum sistem diguna pakai. Amalan pengujian mestilah menurut standard yang semasa serta menepati amalan terbaik dalam industri.

Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat (rujuk A.14.1.1 dan A.14.1.2) dan kepatuhan kepada Polisi Pembangunan Selamat (rujuk A.14.2.1);

(ii) Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan

(iii) Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (*vulnerability scanner*).

10.2.10 *Secure coding*

Peranan: Pentadbir Sistem Aplikasi

Pasukan pembangun sistem perlulah mematuhi amalan terbaik keselamatan pengaturcaraan di persekitaran infrastruktur ICT LLM. Antara amalan terbaik pembangunan kod sumber adalah seperti mengamalkan praktis *Customer Identity and Access Management* (CIAM), *security hardening*, amalan terbaik kawalan akses login dan jaminan kualiti.

A.10.3 DATA UJIAN (*TEST DATA*)

Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian**.**

A.10.3.1 Perlindungan Data Ujian (*Protection of Test Data*)

Peranan: Pengguna, Pentadbir Sistem ICT, ICTSO

Data ujian hendaklah disediakan dengan secukupnya sebelum ujian dilaksanakan. Kaedah menjana data ujian adalah seperti berikut:

(i) Menyediakan secara manual;

(ii) Salin data daripada persekitaran produksi (*productio*n) kepada persekitaran pengujian;

(iii) Salin data ujian daripada sistem aplikasi terdahulu (*legacy*);

(iv) Menyediakan secara automatik seperti perkhidmatan web atau sebarang *tools* yang menjana data; atau

(v) *Back-end Data Injection*.

Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Sebarang prosedur kawalan persekitaran produksi (*production environment*) hendaklah juga dilaksanakan dalam persekitaran pengujian;

(ii) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian;

(iii) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan

(iv) Mengaktifkan audit log bagi merekodkan semua aktiviti pengujian dan pengemaskinian untuk tujuan statistik, pemulihan, keselamatan dan pengesahan data.

BIDANG A.11

HUBUNGAN PEMBEKAL (*SUPPLIER RELATIONSHIP*)

A.11.1 Keselamatan Maklumat Dalam Hubungan Pembekal

(*Information Security in Supplier Relationships*)

A.11.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal

(*Information Security Policy for Supplier Relationships*)

A.11.1.2 Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal

(*Addressing Information Security Within Supplier Agreements*)

A.11.1.3 Rantaian Bekalan Produk ICT

(*Information and Communication Technology Supply Chain*)

A.11.2 Pengurusan Penyampaian Perkhidmatan Pembekal

(*Supplier Service Delivery Management*)

A.11.2.1 Pemantauan dan Kajian Perkhidmatan Pembekal

(*Monitoring and Review Supplier Services*)

A.11.2.2 Pengurusan Perubahan Perkhidmatan Pembekal

(*Managing Changes to Supplier Services*)

A.11.1 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PEMBEKAL (*INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS*)

Objektif: Memastikan aset ICT LLM yang boleh diakses pembekal dilindungi.

A.11.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal (*Information Security Policy for Supplier Relationships*)

Peranan: Pengarah Bahagian, Pemilik Projek dan Pembekal

Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset LLM. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori;

(ii) Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal;

(iii) Mengawal dan memantau akses pembekal;

(iv) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;

(v) Jenis-jenis obligasi kepada pembekal;

(vi) Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat;

(vii) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber LLM kepada pembekal;

(viii) Menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber LLM (LAMPIRAN B)**; dan

(ix) Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.

A.11.1.2 Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal (*Addressing Information Security Within Supplier Agreements*)

Peranan: Syarikat 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 kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak LLM selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.

Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) LLM hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan;

(ii) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan;

(iii) Semua wakil syarikat pembekal hendaklah melepasi tapisan keselamatan daripada agensi berkaitan;

(iv) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;

(v) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;

(vi) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut:

(a) Badan penilai pihak ketiga adalah bebas dan berintegriti;
(b) Badan penilai pihak ketiga adalah kompeten;
(c) Kriteria penilaian;
(d) Parameter pengujian; dan
(e) Andaian yang dibuat berkaitan dengan skop penilaian.

(vii) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan LLM; dan

(viii) Syarikat pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh LLM.

A.11.1.3 Rantaian Bekalan Produk ICT (*Information and Communication Technology Supply Chain*)

Peranan: Pengarah Bahagian, Pembekal dan Pemilik Projek

Perjanjian dengan syarikat 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:

(i) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;

(ii) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk;

(iii) Memastikan jaminan daripada syarikat pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; dan

(iv) Pembekal utama hendaklah memastikan produk atau perkhidmatan yang diberikan adalah selamat daripada unsur-unsur yang boleh mengganggu kelancaran perkhidmatan ICT di LLM.

A.11.2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL (*SUPPLIER SERVICE DELIVERY MANAGEMENT*)

Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.

A.11.2.1 Pemantauan dan Kajian Perkhidmatan Pembekal (*Monitoring and Review Supplier Services*)

Peranan: Pengarah Bahagian, Pembekal dan Pemilik Projek

Prestasi perkhidmatan pembekal hendaklah sentiasa dipantau dan dikaji semula secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:

(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

(iii) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan

(iv) Mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.

A.11.2.2 Pengurusan Perubahan Perkhidmatan Pembekal (*Managing Changes to Supplier Services*)

Peranan: Pengarah Bahagian, Pembekal dan Pemilik Projek

Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut:

(i) Perubahan dalam perjanjian dengan pembekal;

(ii) Perubahan yang dilakukan oleh LLM bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan

(iii) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.

BIDANG A.12

PENGURUSAN INSIDEN KESELAMATAN ICT (*ICT SECURITY INCIDENT MANAGEMENT*)

A.12.1 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan

(*Management of Information Security Incidents and Improvements*)

A.12.1.1 Tanggungjawab dan Prosedur

(*Responsibilities and Procedures*)

A.12.1.2 Pelaporan Kejadian Keselamatan Maklumat

(*Reporting Information Security Events*)

A.12.1.3 Pelaporan Kelemahan Keselamatan Maklumat

(*Reporting Security Weakness*)

A.12.1.4 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat

(*Assessment and Decision on Informaton Security Events*)

A.12.1.5 Tindak Balas Terhadap Insiden Keselamatan Maklumat

(*Response to Information Security Incidents*)

A.12.1.6 Pembelajaran Daripada Insiden Keselamatan Maklumat

(*Learning from Information Security Incidents*)

A.12.1.7 Pengumpulan Bahan Bukti

(*Collection of Evidence*)

A.12.1 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT DAN PENAMBAHBAIKAN (*MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS*)

Objektif: Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan keselamatan.

A.12.1.1 Tanggungjawab dan Prosedur (*Responsibilities and Procedures*)

Peranan: ICTSO, Pengarah Bahagian, CERT LLM dan Pemilik Projek/Sistem Aplikasi

Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden LLM adalah berpandukan Prosedur Operasi Standard (SOP): Prosedur Pengurusan Insiden ICT LLM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Memberikan kesedaran berkaitan Prosedur Pengurusan Insiden ICT LLM dan hebahan kepada warga LLM sekiranya ada perubahan; dan

(ii) Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

A.12.1.2 Pelaporan Kejadian Keselamatan Maklumat (*Reporting Information Security Events*)

Peranan: ICTSO, Pengarah Bahagian, CERT LLM

Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CERT LLM yang kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Insiden keselamatan ICT adalah meliputi perkara-perkara berikut:

(i) Maklumat didapati atau disyaki hilang (serangan virus, kecurian dan lain-lain);
(ii) Maklumat didedahkan kepada pihak yang tidak diberi kuasa;
(iii) Sistem maklumat disyaki digunakan tanpa kebenaran atau disyaki demikian;
(iv) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;
(v) Mekanisme kawalan akses seperti kata laluan dikompromi;
(vi) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
(vii) Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.

Prosedur pelaporan insiden keselamatan siber berdasarkan:

(i) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Keselamatan Teknologi Maklumat dan Komunikasi;
(ii) Surat Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam; dan
(iii) Prosedur Operasi Standard: Prosedur Pengurusan Insiden ICT LLM

A.12.1.3 Pelaporan Kelemahan Keselamatan Maklumat (*Reporting Security Weakness*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM.

Warga LLM dan pembekal yang menggunakan sistem dan perkhidmatan maklumat LLM dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.

A.12.1.4 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat (*Assessment and Decision on Information Security Events*)

Peranan: ICTSO

Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.

A.12.1.5 Tindak Balas Terhadap Insiden Keselamatan Maklumat (*Response to Information Security Incidents*)

Peranan: ICTSO, CERT LLM

Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Prosedur Pengurusan Insiden ICT LLM.

Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut:

(i) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;
(ii) Menjalankan kajian forensik sekiranya perlu;
(iii) Menghubungi pihak yang terlibat dengan secepat mungkin;
(iv) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti;
(v) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
(vi) Menyediakan pelan kontigensi dan mengaktifkan Pelan Kesinambungan Perkhidmatan;
(vii) Menyediakan tindakan pemulihan segera; dan
(viii) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.

A.12.1.6 Pembelajaran Daripada Insiden Keselamatan Maklumat (*Learning from Information Security Incidents*)

Peranan: ICTSO, CERT LLM

Pengetahuan yang diperoleh daripada penganalisaan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya.

Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.

A.12.1.7 Pengumpulan Bahan Bukti (*Collection of Evidence*)

Peranan: ICTSO, CERT LLM

LLM hendaklah menetukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliraharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan yang berkaitan.

BIDANG A.13

ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (*INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT*)

A.13.1 Kesinambungan Keselamatan Maklumat

(*Information Security Continuity*)

A.13.1.1 Perancangan Kesinambungan Keselamatan Maklumat

(*Planning Information Security Continuity*)

A.13.1.2 Pelaksanaan Kesinambungan Keselamatan Maklumat

(*Implementing Information Security Continuity*)

A.13.1.3 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat

(*Verify, Review and Evaluate Information Security Continuity*)

A.13.1.4 ICT *Readiness For Business Continuity*

A.13.2 Lewahan

(*Redundancy*)

A.13.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat

(*Availability of Information Process Facilities*)

A.13.1 KESINAMBUNGAN KESELAMATAN MAKLUMAT (*INFORMATION SECURITY CONTINUITY*)

Objektif: Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan perkhidmatan di LLM.

A.13.1.1 Perancangan Kesinambungan Keselamatan Maklumat (*Planning Information Security Continuity*)

Peranan: Koordinator PKPn, Pasukan Tindak Balas Kecemasan (ERT), Pasukan Pemulihan Bencana ICT

LLM hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, LLM perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi LLM.

LLM juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKPn) LLM;
(ii) Mengenal pasti perkhidmatan kritikal;
(iii) Melaksanakan Penilaian Risiko terhadap perkhidmatan kritikal;
(iv) Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana ICT;
(v) Melaksanakan program kesedaran dan latihan pasukan PKP dan warga LLM;
(vi) Melaksanakan simulasi ke atas pelan di para (c); dan
(vii) Melaksanakan penyelenggaraan ke atas pelan di para (c);

A.13.1.2 Pelaksanaan Kesinambungan Keselamatan Maklumat (*Implementing Information Security Continuity*)

Peranan: Koordinator PKPn, Pasukan Tindak Balas Kecemasan (ERT), Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT

LLM hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Melaksanakan PKPn apabila terdapat gangguan terhadap perkhidmatan kritikal LLM yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini;

(ii) Melaksanakan post-mortem dan mengemaskini pelan-pelan PKPn;

(iii) Mengemas kini pelan-pelan PKPn jika berlaku perubahan kepada fungsi kritikal LLM;

(iv) Mengemas kini struktur tadbir urus PKPn LLM jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan

(v) Memastikan pasukan PKPn mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKPn.

A.13.1.3 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat (*Verify, Review and Evaluate Information Security Continuity*)

Peranan: Pengurusan Atasan LLM, Koordinator PKPn / Pasukan Tindak Balas Kecemasan / Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT / Pemilik Perkhidmatan Kritikal LLM dalam PKPn dan warga LLM

LLM hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.

A.13.1.4 ICT *Readiness For Business Continuity*

LLM hendaklah merancang dan menyediakan Infrastruktur ICT termasuk rangkaian komputer, pelayan, sistem penyimpanan data dan peralatan rangkaian yang boleh diakses bagi menjamin kesinambungan perkhidmatan kepada pelanggan apabila berlaku bencana.

A.13.2 LEWAHAN (*REDUNDANCY*)

Objektif: Untuk memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.

A.13.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat (*Availability of Information Process Facilities*)

Peranan: Pentadbir Pusat Data, Pemilik Perkhidmatan dan Pentadbir Sistem ICT

Kemudahan pemprosesan maklumat LLM perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (*failover test*) keberkesanannya dari semasa ke semasa.

BIDANG A.14

PEMATUHAN (*COMPLIANCE*)

A.14.1 Pematuhan terhadap Keperluan Perundangan dan Kontrak

(*Compliance with Legal and Contractual Requirements*)

A.14.1.1 Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai

(*Identification of Applicable Legislation and Contractual Agreement*)

A.14.1.2 Hak Harta Intelek

(*Intellectual Property Rights*)

A.14.1.3 Perlindungan Rekod

(*Protection of Records*)

A.14.1.4 Privasi dan Perlindungan Maklumat Peribadi

(*Privacy and Protection of Personally Identifiable Information*)

A.14.1.5 Peraturan Kawalan Kriptografi

(*Regulation of Cryptographic Controls*)

A.14.2 Kajian Semula Keselamatan Maklumat

(*Information Security Reviews*)

A.14.2.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali

(*Independent Review of Information Security*)

A.14.2.2 Pematuhan Polisi dan Piawaian Keselamatan

(*Compliance with Security Policies and Standards*)

A.14.2.3 Kajian Semula Pematuhan Teknikal

(*Technical Compliance Review*)

A.14.1 PEMATUHAN TERHADAP KEPERLUAN PERUNDANGAN DAN KONTRAK (*COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS*)

Objektif: Meningkat dan memantapkan tahap keselamatan siber bagi mengelak daripada pelanggaran mana-mana undang-undang, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

A.14.1.1: Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai (*Identification of Applicable Legislation and Contractual Agreement*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di LLM dan pembekal seperti di **LAMPIRAN A.**

A.14.1.2 Hak Harta Intelek (*Intellectual Property Rights*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.

A.14.1.3 Perlindungan Rekod (*Protection of Records*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

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.

A.14.1.4 Privasi dan Perlindungan Maklumat Peribadi (*Privacy and Protection of Personally Identifiable Information*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

LLM hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.

A.14.1.5 Peraturan Kawalan Kriptografi (*Regulation of Cryptographic Controls*)

Peranan: Warga LLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT LLM

Kawalan kriptografi hendaklah dilaksanakan berdasarkan kepada perjanjian kontrak, undang-undang dan peraturan berkaitan.

A.14.2 Kajian Semula Keselamatan Maklumat (*Information Security Reviews*)

Objektif: Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur LLM.

A.14.2.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali (*Independent Review of Information Security*)

Peranan: Pengarah Bahagian dan Pemilik Perkhidmatan

Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.

A.14.2.2 Pematuhan Polisi dan Piawaian Keselamatan (*Compliance with Security Policies and Standards*)

Peranan: Pengarah Bahagian dan Pemilik Perkhidmatan

LLM 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.

A.14.2.3 Kajian Semula Pematuhan Teknikal (*Technical Compliance Review*)

Peranan: Pengarah Bahagian dan Pemilik Perkhidmatan

LLM hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung dalam polisi, piawaian dan keperluan komputer.

LAMPIRAN A

UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Arahan Pentadbiran Ketua Pengarah LLM Bilangan 1 Tahun 2019 ini hendaklah dibaca bersama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuatkuasa antaranya seperti berikut;

1) Arahan Keselamatan;
2) Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
3) Surat Pekeliling Am Bilangan 7 Tahun 2024 - Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
4) Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024;
5) Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024;
6) Surat Pekeliling Am Bilangan 4 Tahun 2022 - Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam;
7) Surat Pekeliling Am Bil. 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam;
8) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
9) Surat Pemakluman Kaedah Pelaksanaan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 6 April 2022;
10) Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team* (GCERT) oleh NACSA bertarikh 28 Januari 2019;
11) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS);

12) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
13) Akta Rahsia Rasmi 1972;
14) Perintah-Perintah Am;
15) Arahan Perbendaharaan;
16) *Standard Operating Procedure* (SOP) ICT LLM;
17) Pelan Kesinambungan Perkhidmatan (PKPn);
18) Tatacara Pengurusan Aset Alih Kerajaan (TPA); dan
19) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)

LAMPIRAN B

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER LLM

Nama (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Bahagian : ……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

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

Tanda tangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....

(Nama Pegawai Keselamatan ICT)

b.p. Ketua Pengarah LLM

Tarikh: .....