POLISI KESELAMATAN SIBER

KEMENTERIAN BELIA DAN SUKAN

VERSI 1.0

POLISI KESELAMATAN SIBER

KEMENTERIAN BELIA DAN SUKAN

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
Nama: Mohd Hazlee bin Ramle Jawatan: *ICT Security Officer* (ICTSO), KBS Tarikh : 28/5/2025	Nama: Noraida binti Mohd Nadzir Jawatan: Pengurus ICT, KBS Tarikh : 28/5/25	Nama: Abdullah bin Hasan Jawatan: *Chief Digital Office* (CDO), KBS Tarikh : 18/6/25

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA	KETERANGAN
19 Mei 2025	1.0	Mesyuarat Jawatankuasa Pemandu ICT Bilangan 2 Tahun 2025	1 Jun 2025	Menggantikan dokumen Dasar Keselamatan ICT (DKICT) Versi 7.1 Tahun 2019

KANDUNGAN

TAKRIFAN

1.	Antivirus	Perisian yang mengimbas virus pada media storan, komputer dan pelayan, seperti cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
2.	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.
3.	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
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 diantara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
7.	BCP/PKP	*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 di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
9.	CIA	*Confidentiality, Integrity, Availability.*
10.	CDO	*Chief Digital Officer* Ketua Pegawai Digital 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 di tempatnya.

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 a 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 a stable destination, such as a 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 dan 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.	*Firewall*	Sistem yang direka bentuk untuk menghalang capaian pengguan yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
20.	*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*).
21.	*CSIRT* KBS	*Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT KBS.
22.	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.

23.	*Hub*	*Hub* merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
24.	ICT	*Information and Communication Technology/* Teknologi Maklumat dan Komunikasi.
25.	ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
26.	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
27.	Impak fungsi jabatan	Melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.
28.	Insiden keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
29.	Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
30.	*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.
31.	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
32.	*Intrusion Detection System* (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian

33.	*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 *maliCDOus code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
34.	ISMS	*Information Security Management System* Sistem Pengurusan Keselamatan Maklumat.
35.	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
36.	KBS	Kementerian Belia dan Sukan.
37.	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
38.	LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
39.	*Lock*	Mengunci komputer.
40.	*Logout*	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
41.	*Malicous Code*	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
42.	*Mobile Code*	*Mobile code* merupakan suatu perisian yang boleh dipindahkan di antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar internet.

43.	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.
44.	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
45.	Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
46.	Pengguna	Warga KBS, pembekal dan pihak-pihak lain yang diberi kebenaran menggunakan perkhidmatan ICT KBS.
47.	Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
48.	Penilaian Risiko	Penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset
49.	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.
50.	*Public-Key Infrastructure* (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perrkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
51.	Pusat Data	Pusat simpanan data
52.	Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar

		kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing
53.	Rahsia besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia
54.	Risiko	Kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian
55.	*Rollback* (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
56.	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.
57.	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
58.	*Server*	Pelayan komputer.
59.	Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memakluan atau kesusahan kepada pentadbiran atau menguntungkan sesebuah kuasa asing
60.	*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.

61.	*Switch*	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense *Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu sistem penghantaran dengan mengurangkan perlanggaran yang berlaku.
62.	Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan
63.	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
64.	*Uninterruptible Power Supply* (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
65.	*Video Conference*	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa yang sama ia diterima oleh penghantar.
66.	*Video Streaming*	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
67.	Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
68.	WAN	*Wide Area Network.* Rangkaian yang merangkumi kawasan yang luas.
69.	Warga KBS	Kakitangan kerajaan yang berkhidmat di KBS, Bahagian, Jabatan dan agensi di bawahnya sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT KBS.
70.	*Wireless LAN*	Jaringan komputer yang terhubung tanpa melalui kabel.

71.	*Worm*	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

TUJUAN

Polisi Keselamatan Siber (PKS), Kementerian Belia dan Sukan (KBS) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS dalam melindungi maklumat.

LATAR BELAKANG

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

OBJEKTIF

Objektif utama polisi ini dibangunkan adalah seperti berikut:

i. menerangkan kepada semua pengguna merangkumi warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat;

ii. memastikan keselamatan sistem penyampaian perkhidmatan KBS ditahap tertinggi dan secara tidak langsung meningkatkan tahap kepercayaan pihak berkepentingan seperti agensi Kerajaan, organisasi dan orang awam;

iii. memastikan kelancaran operasi KBS dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

iv. melindungi kepentingan kepentingan pihak pemegang taruh yang bergantung kepada infrastruktur dan sistem aplikasi dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

v. menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT Kementerian.

ASET ICT KBS

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

c) Maklumat Pengenalan Peribadi ((*Personally Identifiable Information* (PII))

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 Kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan kecuali maklumat PII.

ii. Aliran Data

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

a) Saluran komunikasi dan aliran data antara sistem di KBS;
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 KBS yang dihubungkan dengan sistem KBS. 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 KBS. Contoh perkhidmatan sumber luaran ialah:

a) Perisian Sebagai Satu Perkhidmatan (*Software as a Service* atau SaaS);
b) Platform Sebagai Satu Perkhidmatan (*Platform as a Service* atau PaaS);
c) Infrastruktur Sebagai Satu Perkhidmatan (*Infrastructure as a Service* atau IaaS);
d) Storan Pengkomputeran Awan; dan
e) Pemantauan Keselamatan.

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

PENILAIAN RISIKO DAN KESELAMATAN ICT

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

2. Penilaian risiko keselamatan siber hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan teknologi dan keperluan keselamatan siber KBS.

3. Penilaian ini hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

i. Kerentanan

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

ii. Ancaman

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

iii. Impak

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

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:

1) Teknologi

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

2) Proses

Rekayasa semula (re-engineering) proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

3) 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 KBS hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

1) mengenal pasti kerentanan;
2) mengenal pasti ancaman;
3) menilai risiko;
4) menentukan penguraian risiko;
5) memantau keberkesanan penguraian risiko; dan
6) memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

PRINSIP KESELAMATAN

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

i. Prinsip "Perlu-Tahu"

KBS 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*), KBS hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.
Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

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

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

vi. Pengauditan

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

vii. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan Pelan Pemuliharaan Bencana.

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 (*data at rest*)

Merupakan data yang disimpan dalam pangkalan data, server, backup tape, storan pengkomputeran awan dan lain-lain medium storan.

1) KBS 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.

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

b) Data-dalam-pergerakan (*data in transit*)

Merupakan data yang dihantar antara lokasi atau peranti melalui rangkaian atau internet.

KBS 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 (*data in use*)

Merupakan data yang sedang diakses, diproses atau di kemaskini oleh aplikasi, pengguna atau peralatan.

1) KBS 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.

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

d) Perlindungan Ketirisan Data

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

2) 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, KBS hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (*counter measure*

and 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 hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan seperti di bawah:

a) Peranti Pengkomputeran Peribadi

1) Peranti pengkomputeran peribadi (milik persendirian) merujuk kepada peranti komputer yang digunakan oleh pengguna untuk berinteraksi dengan sistem seperti komputer riba, komputer meja, telefon pintar, tablet dan peranti storan.

2) Pengguna yang menggunakan peranti pengkomputeran peribadi untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada KBS. Walau bagaimanapun, peranti berkenaan hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dibawa masuk ke kawasan terperingkat. Teknologi yang menguruskan peranti berkenaan hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

b) Peranti Rangkaian

1) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti *Virtual Private Network* (VPN) dan kabel.

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-pergerakan dan bagi menghalang ketirisan data.

c) Aplikasi

1) Perisian aplikasi digunakan oleh pengguna untuk memproses dan berinteraksi dengan data seperti pelayan web, pelayan aplikasi dan sistem operasi.

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

d) Pelayan

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

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

e) Persekitaran Fizikal

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

2) KBS hendaklah merujuk kepada CGSO untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

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

4) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

f) Pengkomputeran Awan

1) Pengkomputeran awan merujuk lokasi yang menempatkan sistem ICT menggunakan perkhidmatan pengkomputeran awan yang disediakan melalui internet oleh pihak ketiga dikenali sebagai Penyedia Perkhidmatan Awan (*Cloud Service Provider* (CSP)).

2) JDN dalam persekitaran yang terkawal, selamat, berasaskan standard dan amalan terbaik global telah menyediakan perkhidmatan pengkomputeran awan di Pusat Data Sektor Awam (PDSA) kepada Agensi Sektor Awam yang dikenali sebagai perkhidmatan MyGovCloud@PDSA.

3) Pelaksanaan projek ICT hendaklah menggunakan pengkomputeran awan dengan memberikan keutamaan kepada penggunaan perkhidmatan MyGovCloud@PDSA terutamanya yang melibatkan aplikasi kritikal kerajaan.

4) KBS hendaklah merujuk kepada JDN untuk mendapatkan nasihat mengenai perkhidmatan pengkomputeran awan yang akan dilaksanakan dan mematuhi polisi yang digariskan.

PROSES

Warga KBS 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

a) Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang 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

a) Pindah

1) Pemindahan hak milik aset berlaku dalam keadaan berikut:

- warga KBS meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;
- aset yang dikongsi untuk kegunaan sementara;
- pemberian aset kepada agensi lain; dan
- aset dikembalikan setelah tamat tempoh sewaan.

2) Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (b).

b) Pelupusan

1) Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.

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

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

4) Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

c) Kitaran Hayat

1) Kitaran hayat data hendaklah diuruskan mengikut Akta 629.

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

MANUSIA

Warga KBS, pembekal 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 KBS.

i. Kompetensi Pengguna

a) Kompetensi pengguna termasuk:

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

2) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga KBS berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

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

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

ii. Kompetensi Pelaksana

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

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

1) Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan ICT;
2) Memenuhi keperluan pembelajaran berterusan;
3) Menimba pengalaman yang mencukupi dalam bidang keselamatan siber; dan

4) Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

c) ICTSO yang dilantik oleh KBS hendaklah memenuhi keperluan kompetensi di atas dan bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di KBS.

iii. Peranan Penguna

a) Peranan pengguna hendaklah diberi berdasarkan keperluan dan bidang tugas pengguna.

b) Setiap pegawai yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan 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 KBS yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Kementerian dikembalikan sekiranya berlaku perubahan peranan.

e) Warga KBS yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Kementerian yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Kementerian.

PERNYATAAN POLISI KESELAMATAN SIBER KBS

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

Langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT KBS, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin

timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan. **Sebanyak 14 bidang keselamatan** yang terlibat di dalam PKS KBS diterangkan dengan lebih jelas dan teratur seperti berikut:

BIDANG 01: POLISI KESELAMATAN MAKLUMAT

BIDANG 02: PERANCANGAN BAGI KESELAMATAN ORGANISASI

BIDANG 03: KESELAMATAN SUMBER MANUSIA

BIDANG 04: PENGURUSAN ASET

BIDANG 05: KAWALAN AKSES

BIDANG 06: KRIPTOGRAFI

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

BIDANG 08: KESELAMATAN OPERASI

BIDANG 09: KESELAMATAN KOMUNIKASI

BIDANG 10: PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

BIDANG 11: HUBUNGAN PEMBEKAL

BIDANG 12: PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

BIDANG 13: ASPEK KESELAMATAN BAGI KESINAMBUNGAN PERKHIDMATAN

BIDANG 14: PEMATUHAN

BIDANG 01: POLISI KESELAMATAN MAKLUMAT

1.1 Hala Tuju Pengurusan Untuk Keselamatan Maklumat

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

1.1.1 Polisi Keselamatan Maklumat

Peranan: KSU / CDO / ICTSO / JPICT / Setiausaha/ Pengarah Bahagian

Pelaksanaan polisi ini akan dijalankan oleh Ketua Setiausaha (KSU) KBS yang perlu dipatuhi oleh semua warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS.

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

1.1.2 Kajian Semula Polisi untuk Keselamatan Maklumat

Peranan: CDO / ICTSO / JPICT

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

a. Mengenal pasti dan menentukan perubahan yang diperlukan;

b. Mengemukakan cadangan pindaan untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan;

c. Memaklumkan pindaan yang telah disahkan oleh JPICT kepada warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS; dan

d. Polisi ini hendaklah dikaji semula setiap **LIMA (5) TAHUN SEKALI** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.

BIDANG 02: PERANCANGAN BAGI KESELAMATAN ORGANISASI

2.1 Perancangan Dalaman

Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS KBS.

2.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat

Peranan: Ketua Setiausaha

a. Memastikan penguatkuasaan pelaksanaan Polisi ini;

b. Memastikan warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini;

c. Memastikan semua keperluan KBS seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi;

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

e. Melantik CDO dan ICTSO

Peranan: Ketua Pegawai Maklumat (CDO)

a. Membantu Ketua Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam Polisi ini;

b. Memastikan kawalan keselamatan maklumat dalam KBS diseragam dan diselaraskan dengan sebaiknya;

c. Memastikan Pelan Strategik Pendigitalan KBS mengandungi aspek keselamatan siber; dan

d. Menyelaras pelan latihan dan program kesedaran keselamatan siber.

Peranan: Pegawai Keselamatan ICT (ICTSO)

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

b. Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi dan pekeliling/garis panduan 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 CSIRT KBS dan seterusnya membantu dalam penyiasatan atau pemulihan;

e. Melaporkan insiden keselamatan siber kepada CDO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP);

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

g. Melaksanakan pematuhan Polisi ini oleh warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS;

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

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

Peranan: Setiausaha/ Pengarah Bahagian

a. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu;

b. Pembelian atau peningkatan perisian dan sistem komputer;

c. Perolehan teknologi dan perkhidmatan komunikasi baharu;

d. Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan

e. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi dan pekeliling/garis panduan berkuat kuasa.

Peranan: Ketua Penolong Setiausaha (Cawangan Pembangunan), BPM

a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel 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 dalam Polisi ini;

c. Memantau aktiviti capaian sistem aplikasi;

d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta;

e. Menganalisis dan menyimpan rekod jejak audit;

f. Menyediakan laporan mengenai aktiviti capaian secara berkala; dan

g. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel dalam keadaan yang baik.

Peranan: Ketua Penolong Setiausaha (Cawangan Operasi), BPM

a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;

b. Menentukan ketapan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan dalam Polisi ini;

c. Memantau aktiviti capaian sistem aplikasi dan menyediakan laporan secara berkala;

d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta;

e. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel dalam keadaan yang baik;

f. Mengesan, memantau dan memastikan capaian internet adalah menggunakan sambungan yang sah, stabil dan sentiasa tersedia serta melaporkan kepada Ketua Bahagian sekiranya berlaku penyalahgunaan;

g. Memastikan semua peralatan dan perisian di pusat data diselenggara (konfigurasi dan penambahbaikan) dengan sempurna serta berfungsi dengan baik;

h. Melaksanakan *backup, restore* dan pemulihan ke atas aplikasi, sistem pengoperasian server, pangakalan data dan lain-lain yang berkaitan;

i. Melaksanakan pengurusan Pusat Data KBS; dan

j. Melaporkan sebarang insiden keselamatan siber kepada CDO.

Peranan: Jawatankuasa Pemandu ICT (JPICT)

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

Peranan: *Cyber Security Incident Response Team (*CSIRT*) KBS* KBS

Peranan dan tanggungjawab CSIRT seperti yang terkandung dalam Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bagi mengurus dan mengendalikan insiden keselamatan siber.

Peranan: Pengguna / Warga KBS

a. Membaca, memahami dan mematuhi Polisi ini;

b. Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya;

c. Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat;

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

e. Melaksanakan langkah-langkah perlindungan seperti yang berikut:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan maklumat;
v. Mematuhi polisi, piawaian dan garis panduan keselamatan siber yang ditetapkan;
vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum.

f. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT KBS dengan segera;

g. Menghadiri program-program kesedaran mengenai keselamatan siber;

h. Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini; dan

i. Menandatangani **Surat Akuan Pematuhan PKS KBS (LAMPIRAN 1)**;

Peranan: Bahagian Pengurusan Maklumat (BPM)

Membangun serta menyebarkan polisi dan langkah-langkah keselamatan siber kepada Warga KBS.

2.1.2 Pengasingan Tugas

Peranan: Setiausaha/ 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 ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi;
c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan

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

2.1.3 Hubungan Dengan Pihak Berkuasa

Peranan : CSIRT KBS

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

a. Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab KBS;

b. Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang perlu dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM). Pihak yang

dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan

c. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.

2.1.4 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus

Peranan : **Pengguna**

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

a. Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;

b. Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini;

c. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan

d. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

2.1.5 Keselamatan Maklumat dalam Pengurusan Projek

Peranan : Pengguna

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

a. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek KBS;

b. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;

c. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;

d. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS KBS; dan

e. Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.

2.2 Peranti Mudah Alih, Telekerja Dan Mesyuarat Dalam Talian

Objektif : Memastikan keselamatan telekerja, mesyuarat dalam talian dan penggunaan peralatan mudah alih.

2.2.1 Polisi Peranti Mudah Alih

Peranan : **Bahagian Pengurusan Maklumat (BPM)**

Membangun serta menyebarkan polisi dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul berkaitan penggunaan peranti mudah alih.

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

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

Peranan : **Warga KBS**

Perkara-perkara yang perlu dipatuhi:

a. Pendaftaran ke atas peralatan mudah alih;
b. Keperluan ke atas perlindungan secara fizikal;
c. Kawalan ke atas pemasangan perisian peralatan mudah alih;
d. Kawalan ke atas versi dan *patches* perisian;
e. Sekatan ke atas akses perkhidmatan maklumat secara dalam talian;

f. Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan
g. Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.

2.2.2 Telekerja (*Teleworking*)

Peranan : Warga KBS

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

b. Kawalan capaian dijalankan bergantung kepada kategori pengguna, sensitiviti aplikasi dan jenis data yang dicapai dan tetapan mudah alih dan telekerja.

c. Capaian maklumat dan aplikasi di pusat data melalui jarak jauh (*remote access*) adalah terhad kepada pengguna yang dibenarkan sahaja dan mestilah melalui *Virtual Private Network* (VPN) yang dibenarkan.

d. Penggunaan perkhidmatan ini hendaklah mendapatkan kebenaran ICTSO. Pengguna yang diberikan hak adalah dipertanggungjawab penuh ke atas penggunaan kemudahan ini.

2.2.3 Mesyuarat Dalam Talian

Peranan : Penyelaras/ Pentadbir Mesyuarat

Mesyuarat dalam talian hendaklah mengadaptasi teknik yang selamat seperti penggunaan kata laluan sebelum dibenarkan terlibat di dalam mesyuarat berkenaan.

Peranan : Warga KBS

a. Polisi dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, dibincang atau disimpan semasa mesyuarat dalam talian.

b. Menggunakan platform yang sah dan dibenarkan sahaja.

BIDANG 03: KESELAMATAN SUMBER MANUSIA

3.1 Sebelum Perkhidmatan

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

3.1.1 Tapisan Keselamatan

Peranan : Pengguna

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

a. menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan

b. menjalankan tapisan keselamatan untuk warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

3.1.2 Terma dan Syarat Perkhidmatan

Peranan : Pengguna

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

a. menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS yang terlibat dalam menjamin keselamatan aset ICT; dan

b. mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

3.2 Dalam Tempoh Perkhidmatan

Objektif :

Memastikan warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS 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.

3.2.1 Tanggungjawab Pengurusan

Peranan : Pengguna dan ICTSO

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

3.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat

Peranan : Pengguna

Warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS 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 berikut:

a. memastikan kesedaran, pendidikan dan latihan yang berkaitan PKS KBS, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;

b. memastikan kesedaran yang berkaitan PKS KBS perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan

c. memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

3.2.3 Proses Tatatertib

Peranan : Setiausaha Bahagian BKP

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

a. memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga KBS sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh KBS; dan

b. warga KBS yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT KBS.

3.3 Penamatan dan Pertukaran Perkhidmatan

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

3.3.1 Penamatan atau Pertukaran Tanggung Jawab Perkhidmatan

Peranan : Warga KBS dan Bahagian Pengurusan Maklumat

Warga KBS yang telah **tamat perkhidmatan** hendaklah:

a. memastikan semua aset ICT dikembalikan kepada KBS mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;

b. membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan KBS dan/atau terma perkhidmatan yang ditetapkan; dan

c. maklumat rasmi KBS dalam peranti tidak dibenarkan dibawa keluar dari KBS.

Warga KBS yang telah **bertukar perkhidmatan** hendaklah:

a. Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada KBS mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

b. Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.

BIDANG 04: PENGURUSAN ASET

4.1 Tanggungjawab Terhadap Aset

Objektif : Mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KBS.

4.1.1 Inventori Aset

Peranan : Pegawai Aset / BPM / Warga KBS

Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT KBS. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:

a. KBS hendaklah mengenal pasti Pegawai Aset di setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT;

b. memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa;

c. memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan

d. Pegawai Aset hendaklah mengesahkan penempatan aset ICT.

4.1.2 Pemilikan Aset

Peranan : Pegawai Aset / BPM / Warga KBS

Aset yang diselanggara hendaklah hak milik KBS. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut:

a. memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset;

b. memastikan aset telah dikelaskan dan dilindungi;

c. kenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;

d. memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan

e. memastikan semua jenis aset dipelihara dengan baik.

4.1.3 Penggunaan Aset yang Dibenarkan

Peranan : Pengguna

Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.

4.1.4 Pemulangan Aset

Peranan : Pengguna

Memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan selepas bersara, bertukar kementerian dan penamatan perkhidmatan atau kontrak.

4.2 Pengelasan Maklumat

Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

4.2.1 Pengelasan Maklumat

Peranan : Pegawai Pengelas

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

4.2.2 Pelabelan Maklumat

Peranan : Pengguna

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

4.2.3 Pengendalian Aset

Peranan : Pengguna

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

a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

b. memeriksa dan menentukan maklumat adalah 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, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

g. menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

4.3 Pengendalian Media

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

4.3.1 Pengurusan Media Boleh Alih

Peranan : Pentadbir Sistem ICT dan Pengguna

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

a. melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;

b. mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;

c. mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;

d. mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan

e. menyimpan semua jenis media di tempat yang selamat.

4.3.2 Pelupusan Media

Peranan : Pentadbir Sistem ICT

a. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan

b. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.

4.3.3 Pemindahan Media Fizikal

Peranan : Pentadbir Sistem ICT

a. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan

b. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.

BIDANG 05: KAWALAN AKSES

5.1 Kawalan Akses

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

5.1.1 Polisi Kawalan Akses

Peranan : CDO, ICTSO dan Pentadbir Sistem ICT

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

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

i. keperluan keselamatan aplikasi;
ii. hak akses dan polisi 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; dan
viii. pembatalan hak akses;

c. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan

d. Capaian *privilege*.

5.1.2 Capaian kepada Rangkaian dan Perkhidmatan Rangkaian

Peranan : ICTSO, Pentadbir Rangkaian dan Pentadbir Operasi ICT

Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian oleh Pentadbir Rangkaian setelah mendapat pengesahan daripada Ketua Bahagian/Jabatan masing-masing. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

a. menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian KBS, rangkaian agensi lain dan rangkaian awam;

b. mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan

c. memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

5.2 Pengurusan Akses Pengguna

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

5.2.1 Pendaftaran dan Penamatan Pengguna

Peranan : Pengguna, BPM dan Pemilik Sistem / Portal

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

a. akaun yang diperuntukkan oleh KBS sahaja boleh digunakan;

b. akaun pengguna mestilah unik;

c. sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;

d. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertaklik kepada peraturan yang berkuatkuasa. Akaun boleh ditarik balik jika didapati terdapat penyalahgunaan atau pelanggaran peraturan;

e. penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan

f. menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan KBS.

5.2.2 Peruntukan Akses Pengguna

Peranan : Pentadbir Sistem ICT dan KPSU BPM

Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT berdasarkan skop tugas serta garis panduan yang berkuat kuasa.

5.2.3 Pengurusan Hak Akses Istimewa

Peranan : Pentadbir Sistem ICT

a. Peruntukan dan penggunaan hak akses istimewa hendaklah dihad dan dikawal; dan

b. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada Prosedur Pendaftaran dan Penamatan Pengguna.

5.2.4 Pengurusan Maklumat Pengesahan Rahsia Pengguna

Peranan : ICTSO dan Pentadbir Sistem ICT

a. Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal; dan

b. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.

5.2.5 Kajian Semula Hak Akses Pengguna

Peranan : ICTSO dan Pentadbir Sistem ICT

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

b. Pentadbir Sistem ICT perlu mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.

5.2.6 Pembatalan atau Pelarasan Hak Akses

Peranan : Setiausaha / Pengarah Bahagian, Pentadbir Sistem ICT

Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam KBS.

5.3 Tanggungjawab Pengguna

Objektif : Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.

5.3.1 Penggunaan Maklumat Pengesahan Rahsia

Peranan : Setiausaha / Pengarah Bahagian, ICTSO, Pentadbir Sistem ICT dan Pengguna

a. Membaca, memahami dan mematuhi PKS KBS;

b. Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;

c. Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat KBS;

d. Melaksanakan langkah-langkah perlindungan seperti yang berikut:

i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
iii. menentukan maklumat sedia untuk digunakan;
iv. mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
v. memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vi. menjaga kerahsiaan daripada diketahui umum.

e. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera;

f. Menghadiri program-program kesedaran mengenai keselamatan siber; dan

g. Mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.

5.4 Kawalan Akses Sistem dan Aplikasi

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

5.4.1 Sekatan Akses Maklumat

Peranan : **ICTSO, Pentadbir Sistem ICT dan Pengguna**

Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut polisi kawalan akses yang telah ditentukan.

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

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 berikut:

a. mengesahkan pengguna yang dibenarkan selaras dengan peraturan KBS;

b. mewujudkan kata laluan yang berkualiti;

c. menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem;

d. mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin;

e. mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna;

f. mewujudkan sistem pengurusan kata laluan berkualiti; dan

g. mewujudkan jejak audit ke atas semua capaian aplikasi sistem.

5.4.3 Sistem Pengurusan Kata Laluan

Peranan : Setiausaha / Pengarah Bahagian, ICTSO, Pentadbir Sistem ICT dan Pengguna

Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KBS seperti berikut:

a. kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

b. kata laluan hendaklah ditukar apabila disyaki berlaku kebocoran kata laluan atau dikompromi;

c. 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;

d. kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun;

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

f. kata laluan tidak boleh dipaparkan semasa input, dalam laporan atau media lain dan dikodkan di dalam atur cara;

g. penguatkuasaan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas kata laluan diset semula;

h. kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

i. had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan

j. sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.

5.4.4 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa

Peranan : ICTSO dan Pentadbir Sistem ICT

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

5.4.5 Kawalan Akses Kepada Kod Sumber Program

Peranan : Pentadbir Sistem ICT, Pemilik Sistem dan Bahagian Pengurusan Maklumat (BPM)

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

a. log audit perlu dikekalkan kepada semua akses kepada kod sumber;

b. penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan

c. kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik KBS.

BIDANG 06: KRIPTOGRAFI

6.1 Kawalan Kriptografi

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

6.1.1 Polisi Penggunaan Kawalan Kriptografi

Peranan : Pengguna

Kriptografi merangkumi kaedah-kaedah seperti berikut:

a. Enkripsi

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

b. Tandatangan Digital

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

6.1.2 Pengurusan Kunci Awam

Peranan : Pentadbir sistem ICT, Warga KBS

Pengurusan ke atas Infrastruktur Perkhidmatan Prasarana 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. Perkara yang perlu dipatuhi adalaah seperti berikut:

a. penggunaan sigil digital hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;

b. sijil digital hendaklah disimpan di tempat yang selamat bagi mengelakkan kecurian atau disalahguna;

c. perkongsian sijil digital untuk sebarang capaian sistem adalah tidak dibenarkan; dan

d. sebarang perubahan kepada pemilik atau kehilangan/kerosakan perlu dilaporkan kepada pentadbir sistem.

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

7.1 Kawasan Selamat

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

7.1.1 Perimeter Keselamatan Fizikal

Peranan : Setiausaha / Pengarah Bahagian

Bertujuan menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT. Perkara-perkara yang perlu dipatuhi seperti berikut:

a. kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;

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

c. melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;

d. mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;

e. mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia;

f. melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad;

g. memastikan kawasan penghantaran dan pemunggahan dan juga tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan

h. memasang alat penggera atau kamera keselamatan.

7.1.2 Kawalan Kemasukan Fizikal

Peranan : Pengguna, Bahagian Khidmat Pengurusan (BKP)

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

a. pas keselamatan hendaklah dipamerkan sepanjang waktu bertugas atau berada di premis KBS;

b. setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan dikembalikan semula selepas tamat lawatan;

c. hanya pengguna yang diberi kebenaran boleh menggunakan aset ICT KBS;

d. warga KBS perlu mengembalikan pas keselamatan kepada BKP apabila bertukar, tamat perkhidmatan atau bersara dalam tempoh/seperti garis panduan/tatacara daripada BKP; dan

e. kehilangan pas keselamatan hendaklah dilaporkan segera kepada Pihak Berkuasa.

7.1.3 Keselamatan Pejabat, Bilik dan Kemudahan

Peranan : Pengguna

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

a. kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran;

b. kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan

c. petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi Arahan Keselamatan yang berkuatkuasa.

7.1.4 Perlindungan Daripada Ancaman Luar Dan Persekitaran

Peranan : Setiausaha/ Pengarah Bahagian, Bahagian Khidmat Pengurusan (BKP)

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

7.1.5 Bekerja di Kawasan Selamat

Peranan : Setiausaha/ Pengarah Bahagian, Bahagian Khidmat Pengurusan (BKP)

a. Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan.

b. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga KBS yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis KBS termasuklah Pusat Data.

c. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam.

d. Kawalan keselamatan ke atas kawasan tersebut adalah seperti 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 KBS yang telah diberi kuasa sahaja dan dipantau pada setiap masa;
   iii. pemantauan dibuat menggunakan CCTV kamera atau lain-lain peralatan yang sesuai;

iv. peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual atau apabila berlaku sebarang pencerobohan;
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.

7.1.6 Kawasan Penyerahan dan Pemunggahan

Peranan : Pengguna

a. 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; dan

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

7.2 Peralatan ICT

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

7.2.1 Penempatan dan Perlindungan Peralatan ICT

Peranan : Warga KBS

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 berikut:

a. penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

b. warga KBS bertanggungjawab sepenuhnya ke atas perkakasan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

c. warga KBS dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

d. warga KBS dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;

e. warga KBS perlu memastikan komputer/komputer riba yang dibekalkan dilengkapi dengan perisian *antivirus.* Perisian berkenaan perlu sentiasa aktif (*activated*), dikemaskini dan versi terkini di samping sentiasa melakukan imbasan ke atas media storan yang digunakan;

f. semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna;

g. warga KBS adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah penempatannya;

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

i. semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;

j. peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci;

k. semua perkakasan ICT yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

l. perkakasan ICT yang dibawa ke luar premis KBS, perlu mendapat kelulusan Pegawai Aset dan direkodkan mengikut pekeliling perbendaharaan yang berkuatkuasa bagi tujuan pemantauan;

m. kehilangan perkakasan ICT di luar waktu pejabat perlu dikendalikan mengikut pekeliling perbendaharaan yang berkuatkuasa;

n. semua pergerakan peralatan ICT perlu direkodkan atau dikemaskini mengikut peraturan semasa yang berkuat kuasa;

o. pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

p. warga KBS tidak dibenar mengubah kedudukan perkakasan ICT dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

q. sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih;

r. 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;

s. konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang telah ditetapkan;

t. tidak memuat turun dan memasang perisian tanpa lesen yang sah dan kebenaran Pentadbir Sistem ICT;

u. warga KBS dilarang sama sekali mengguna dan mengubah kata laluan pentadbir (*administrator password)* yang telah ditetapkan; dan

v. warga KBS bertanggungjawab terhadap peralatan ICT di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi sahaja.

7.2.2 Utiliti Sokongan

Peranan : Bahagian Khidmat Pengurusan (BKP), Pentadbir Sistem ICT

a. Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan;

b. Peralatan sokongan yang bersesuaian boleh digunakan bagi perkhidmatan kritikal seperti di pusat data supaya mendapat bekalan kuasa yang berterusan; dan

c. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).

7.2.3 Keselamatan Kabel

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 berikut:

a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;

b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;

c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

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

7.2.4 Penyelenggaraan Peralatan

Peranan : Setiausaha/ Pengarah Bahagian, Pentadbir Sistem ICT

a. Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan, keutuhan yang berterusan, kerahsiaan dan integriti.

b. Langkah-langkah keselamatan yang perlu diambil termasuk seperti yang berikut:

i. bertanggungjawab terhadap penyelenggaraan setiap perkakasan ICT 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 serta mendapat kebenaran daripada Pentadbir Sistem ICT;
iv. menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;
v. semua aktiviti penyelenggaraan perlu direkodkan; dan
vi. memaklumkan kepada pengguna yang terlibat sebelum melaksanakan aktiviti penyelenggaraan berkala atau atas keperluan.

7.2.5 Keselamatan Peralatan dan Aset di Luar Premis

Peranan : Warga KBS

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

a. Peralatan perlu dilindungi dan dikawal sepanjang masa;

b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan

c. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.

7.2.6 Pelupusan yang Selamat atau Penggunaan Semula Peralatan

Peranan : Pentadbir Sistem ICT, Pegawai Aset, Warga KBS

a. 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.

b. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KBS.

c. 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 KBS. Langkah-langkah seperti berikut hendaklah diambil:

   i. 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 ICT yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan dan 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. warga KBS adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:
      1. menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;
      2. mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *Central Processing Unit* (CPU) seperti *Random Access Memory* (RAM), *Hardisk*, *Motherboard* dan sebagainya;
      3. menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana Bahagian di KBS;
      4. memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan
      5. melupuskan sendiri peralatan ICT dan tidak mematuhi tatacara pelupusan semasa yang berkuat kuasa.

d. Warga KBS 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;

e. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal dan selamat; Sekiranya maklumat perlu disimpan, maka warga KBS dibenar untuk membuat salinan;

f. Warga KBS perlu memastikan pelupusan perkakasan ICT yang mengandungi data dan maklumat berstatus terperingkat perlu mematuhi Buku Arahan Keselamatan (Semakan dan Pindaan 2017) dan Garis Panduan Sanitasi Media Elektronik Sektor Awam;

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

h. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan

i. Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Pemantauan Aset.

7.2.7 Peralatan Pengguna Tanpa Kawalan

Peranan : Warga KBS

a. Warga KBS hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya; dan

b. Warga KBS perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:

c. Menamatkan sesi penggunaan (*log out*) apabila selesai tugas;

d. *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan

e. Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.

7.2.8 Polisi Meja Kosong dan Skrin Kosong (*Clear Desk* dan *Clear Screen*)

Peranan : Warga KBS

a. Polisi meja kosong untuk kertas dan media penyimpanan boleh alih serta polisi skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan.

b. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

c. *Clear desk* dan *clear screen* 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 berikut:

   i. menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer/ komputer riba;
   ii. menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;
   iii. memastikan semua dokumen diambil segera dari 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.

BIDANG 08: KESELAMATAN OPERASI

8.1 Prosedur dan Tanggungjawab Operasi

Objektif : Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat.

8.1.1 Prosedur Operasi yang Didokumenkan

Peranan : Pentadbir Operasi ICT

Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut:

a. Semua prosedur keselamatan siber yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;

b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan

c. Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.

8.1.2 Pengurusan Perubahan

Peranan : Pentadbir Operasi ICT, Pengguna

Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut:

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

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

c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan

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

8.1.3 Pengurusan Kapasiti

Peranan : Pentadbir Operasi 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 berikut:

a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan

b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

8.1.4 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi

Peranan : Pentadbir Operasi ICT, 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 berikut:

a. Perkakasan, rangkaian dan perisian yang digunakan bagi tugas membangun, mengemas kini, dan menguji aplikasi hendaklah diasingkan dari perkakasan, rangkaian dan perisian yang digunakan dalam persekitaran pembangunan (*development*), pengujian (*testing*), persediaan (*staging*) dan persekitaran sebenar (*production*).

b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah dilakukan oleh pegawai yang berlainan bagi mengelakkan capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan

c. Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

8.2 Perlindungan Daripada Perisian Hasad

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

8.2.1 Kawalan Daripada Perisian Hasad

Peranan : Pentadbir Operasi ICT, Pengguna

Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut:

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

b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;

c. Mengimbas semua perisian, sistem dan media storan dengan antivirus sebelum menggunakannya;

d. Mengemas kini antivirus dengan *signature/pattern* antivirus yang terkini;

e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; dan

h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.

8.3 Penduaan (*Backup*)

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

8.3.1 Sandaran Maklumat

Peranan : Pentadbir Sistem ICT

a. Salinan penduaan maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur penduaan yang dipersetujui; dan

b. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, penduaan hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off site*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Membuat penduaan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
ii. Membuat penduaan ke atas semua data dan maklumat mengikut keperluan operasi;
iii. Menguji sistem penduaan sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan
iv. penduaan hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara **harian, mingguan, bulanan** atau **tahunan**. Kekerapan penduaan bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya **TIGA (3) GENERASI.**

8.4 Pengelogan dan Pemantauan

Objektif : Merekodkan peristiwa dan menghasilkan bukti.

8.4.1 Pengelogan Kejadian

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

a. Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap;

b. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem;

c. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan;

d. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data;

e. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: dan

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*).

f. Perkara-perkara berikut hendaklah dilaksanakan:

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; dan
iii. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO.

8.4.2 Perlindungan Maklumat Log

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

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

8.4.3 Log pentadbir dan Pengendali

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini seperti berikut:

a. Memantau penggunaan kemudahan memproses maklumat secara berkala;

b. Aktiviti log hendaklah dilindungi, direkodkan dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu;

c. Kesalahan, kesilapan dan/ atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;

d. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan

e. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, hendaklah melaporkan kepada ICTSO.

8.4.4 Penyeragaman Jam

Peranan : Pentadbir Operasi ICT

Waktu bagi semua sistem pemprosesan maklumat yang berkaitan dalam domain KBS atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal iaitu *National Metrology Institute of Malaysia* (NMIM).

8.5 Kawalan Perisian yang Beroperasi

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

8.5.1 Pemasangan Perisian Pada Sistem yang Beroperasi

Peranan : Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Operasi ICT

Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan ICTSO adalah seperti berikut:

a. Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;

b. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan

c. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT;

d. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

8.6 Pengurusan Kerentanan Teknikal

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

8.6.1 Pengurusan Kerentanan Teknikal

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

Pengurusan Kerentanan Teknikal ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:

a. Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;

b. Menganalisis tahap risiko kerentanan; dan

c. Mengambil tindakan pengolahan dan kawalan risiko.

8.6.2 Sekatan ke atas Pemasangan Perisian

Peranan : Pentadbir Operasi ICT, Pengguna

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

a. Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan pengguna dan pembekal KBS.

b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan

c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.

8.7 Pertimbangan Tentang Audit Sistem Maklumat

Objektif : Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.

8.7.1 Kawalan Audit Sistem Maklumat

Peranan : ICTSO, Pentadbir Sistem ICT, Pentadbir Operasi ICT

Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perkhidmatann di KBS.

BIDANG 09: KESELAMATAN KOMUNIKASI

9.1 Pengurusan Keselamatan Rangkaian

Objektif : Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

9.1.1 Kawalan Rangkaian

Peranan : Setiausaha/ Pengarah Bahagian, ICTSO, Pentadbir Operasi ICT

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

a. bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan;

b. peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk;

c. capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;

d. semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;

e. tembok api hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian;

f. semua trafik keluar dan masuk rangkaian hendaklah melalui tembok api di bawah kawalan KBS;

g. semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna **KECUALI** mendapat kebenaran daripada ICTSO;

h. memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat KBS;

i. memasang *Web Content Filtering* pada *Internet Gateway* atau kawalan capaian internet yang bersesuaian untuk menyekat aktiviti/capaian yang dilarang;

j. semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di KBS sahaja dan penggunaan selainnya adalah dilarang sama sekali;

k. kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya;

l. semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan;

m. menempatkan atau memasang antara muka (interfaces) yang bersesuaian di antara rangkaian KBS, rangkaian agensi lain dan rangkaian awam;

n. menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian di antara rangkaian KBS, rangkaian agensi lain dan rangkaian awam;

o. mewujudkan, memantau dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan

p. mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan (capaian jarak jauh);

9.1.2 Keselamatan Perkhidmatan Rangkaian

Peranan : Setiausaha/ Pengarah Bahagian, Pentadbir Operasi ICT, Pembekal

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

9.1.3 Pengasingan Dalam Rangkaian

Peranan : Pentadbir Operasi ICT

Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna, sistem maklumat dan agensi di bawah KBS mengikut segmen yang berbeza.

9.2 Pemindahan Data dan Maklumat

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

9.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat

Peranan : Pentadbir Operasi ICT, Pentadbir Sistem ICT, Pembekal

Perkara yang perlu dipatuhi adalah seperti berikut:

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

b. Terma pemindahan data, maklumat dan perisian antara KBS dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;

c. Media yang mengandungi maklumat perlu dilindungi;

d. Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat KBS; dan

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

9.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat

Peranan : ICTSO, Pentadbir Operasi ICT, Pentadbir Sistem ICT

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

a. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat KBS;

b. Polisi, prosedur dan kawalan penghantaran dan penerimaan maklumat yang formal perlu diwujudkan untuk melindungi maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; dan

d. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan dan penerimaan.

9.2.3 Pengurusan Mel Elektronik (e-mel)

Peranan : Pengguna

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:

a. Akaun atau alamat Mel elektronik (e-mel) yang diperuntukkan oleh KBS sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

b. Penghantaran dan penerimaan dokumen rasmi hendaklah menggunakan e-mel rasmi KBS dan direkod ke dalam DDMS 2.0;

c. Mengehadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan e-mel *bombing*;

d. pengemaskinian e-mel hendaklah dibuat sekiranya mailbox pengguna tidak aktif selama tiga (3) bulan kecuali menerima pemakluman rasmi bagi mengesahkan pengguna mailbox masih aktif;

e. penghantaran lampiran dalam format atau extension “*.exe, *.bat” dan “ *.com” tidak dibenarkan;

f. Sebarang pengemaskinian status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke KBS) perlu dimaklumkan kepada Pentadbir Operasi ICTdalam tempoh 30 hari;

g. Pengguna ICT KBS hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.

h. Menggunakan kaedah enkripsi (*encryption*) bagi dokumen terperingkat yang dihantar secara elektronik; dan

i. Penghantaran fail bersaiz besar menggunakan platform *Google Drive* yang disediakan oleh Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (*MyGovUC*).

9.2.4 Perjanjian Kerahsiaan atau Ketakdedahan

Peranan : ICTSO, Setiausaha/Pengarah Bahagian, Pentadbir Operasi ICT, Pembekal

a. Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan; dan

b. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat seperti berikut.

i. PKS KBS;
ii. Tapisan Keselamatan;
iii. Perakuan Akta Rahsia Rasmi 1972; dan
iv. Hak Harta Intelek.;

BIDANG 10: PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

10.1 Keperluan Keselamatan Sistem Maklumat

Objektif : Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang seluruh kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan dalam rangkaian awam.

10.1.1 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat

Peranan : Pentadbir Sistem ICT

Keperluan keselamatan maklumat hendaklah dimasukkan bagi pembangunan dan sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada dengan mematuhi perkara-perkara berikut:

a. 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;

b. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan PKS KBS;

c. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan

d. Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.

10.1.2 Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam (*Securing Application Services on Public Networks*)

Peranan : Pentadbir Operasi ICT

Perkara yang perlu dipertimbangkan adalah seperti berikut:

a. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi KBS;

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

c. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (authentication);

d. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;

e. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan

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

10.1.3 Melindungi Transaksi Perkhidmatan Aplikasi (*Protection Application Services Transactions*)

Peranan : ICTSO, Setiausaha/ Pengarah Bahagian, Pentadbir Sistem ICT, Pentadbir Operasi 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 (*reply message*) yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut:

a. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;

b. Memastikan semua aspek transaksi seperti di bawah dipatuhi:

   i. Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan;
   ii. Mengekalkan kerahsiaan maklumat;
   iii. Mengekalkan privasi pihak yang terlibat; dan

iv. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi.

c. Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.

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.

10.2.1 Polisi Pembangunan Selamat (*Secure Development Policy*)

Peranan : Pentadbir Sistem ICT

Pembangunan perisian dan sistem aplikasi perlu dilaksanakan mengikut keperluan dan ianya hendaklah dikaji dan disemak secara berkala untuk memastikan keberkesanannya.

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

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut:

a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;

b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal;

c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

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

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

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

Apabila platform operasi berubah, aplikasi utama bisnes hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti berikut:

a. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; dan

b. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan.

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

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja.

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

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

Prinsip bagi sistem keselamatan kejuruteraan hendaklah berpandukan kepada **Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V)** sektor awam yang terkini untuk apa-apa usaha pelaksanaan sistem maklumat.

10.2.6 Persekitaran Pembangunan Selamat (*Secure Development Environment*)

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

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

b. KBS 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 boleh dipercayai; dan
vi. kawalan ke atas capaian kepada persekitaran pembangunan sistem.

10.2.7 Pembangunan oleh Khidmat Luaran (*Outsourced Software Developments*)

Peranan : Pentadbir Sistem ICT, Pentadbir Operasi ICT

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

a. Perkiraan perlesenan, kod sumber ialah **HAK MILIK** KBS dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*;

b. Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori **"Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko"**;

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

d. Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; dan

e. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.

10.2.8 Pengujian Keselamatan Sistem (*System Security Testing*)

Peranan : ICTSO, Pentadbir Sistem ICT, Pentadbir Operasi ICT

Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti berikut:

a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;

b. Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat;

c. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan; dan

d. Aktiviti pengujian keselamatan sistem hendaklah dilaksanakan atas sistem baharu, tambah baik, naik taraf dan versi baharu berdasarkan *Security Posture Assessment* (SPA) yang telah ditetapkan berdasarkan keperluan.

10.2.9 Pengujian Penerimaan Sistem (*System Accepting Testing*)

Peranan : Pentadbir Sistem ICT, Pengguna

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 berikut:

a. Pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat (rujuk 10.1.1 dan 10.1.2) dan kepatuhan kepada Polisi Pembangunan Selamat (rujuk 10.2.1); dan

Peranan : Pentadbir Sistem ICT, Pengguna

b. Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai;

10.3 Data Ujian (*Test Data*)

Objektif : Memastikan perlindungan ke atas data yang digunakan untuk pengujian.

10.3.1 Perlindungan Data Ujian

Peranan : ICTSO, Pentadbir Sistem ICT, Pengguna

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

a. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian;

b. Pentadbir Sistem ICT yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian;

c. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan

d. Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.

BIDANG 11: HUBUNGAN PEMBEKAL

11.1 Keselamatan Maklumat Dalam Hubungan Pembekal

Objektif : Memastikan aset ICT KBS yang boleh dicapai oleh pembekal dilindungi.

11.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal

Peranan : Setiausaha/ Pengarah Bahagian, Pembekal

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

a. mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori;

b. proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal;

c. mengawal dan memantau akses pembekal;

d. keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;

e. jenis-jenis obligasi kepada pembekal;

f. pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat;

g. pembekal perlu mematuhi Arahan Keselamatan yang berkuatkuasa; dan

h. menandatangani Surat Akuan Pematuhan PKS KBS (Lampiran 3) dan Perakuan Akta Rahsia Rasmi 1972 sebagaimana (Lampiran 4).

11.1.2 Menangani Keselamatan Dalam Perjanjian Pembekal

Peranan : Pembekal

a. 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;

b. Pembekal hendaklah memastikan kakitangan mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada KBS selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa;

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

i. KBS hendaklah memilih pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam kod bidang yang berkaitan;
ii. pembekal yang mempunyai sijil keselamatan yang berkaitan perkhidmatan akan diberi keutamaan sekiranya perlu;
iii. pembekalan atau perkhidmatan yang ditawarkan hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;
iv. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh pembekal;
v. laporan penilaian pihak ketiga yang dikemukakan oleh pembekal hendaklah disemak berdasarkan faktor-faktor seperti berikut:
   a) badan penilai pihak ketiga adalah bebas dan berintegriti;
   b) badan penilai pihak ketiga adalah kompeten;
   c) kriteria penilaian;
   d) parameter pengujian;
   e) andaian yang dibuat berkaitan dengan skop penilaian;
vi. pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan KBS; dan

vii. pembekal hendaklah mematuhi pengelasan maklumat yang telah ditetapkan.

11.1.3 Rantaian Bekalan Teknologi Maklumat dan Komunikasi

Peranan : Setiausaha/ Pengarah Bahagian, Pembekal

Perjanjian dengan pembekal hendaklah mengandungi keperluan keselamatan ICT yang dikaitkan dengan pembekalan dan perkhidmatan. Perkara-perkara yang perlu diambil kira adalah seperti berikut:

a. memastikan keperluan keselamatan ICT diambilkira dalam projek pembekalan dan perkhidmatan;

b. pembekal hendaklah memaklumkan keperluan keselamatan ICT kepada pihak ketiga atau subkontraktor berkaitan projek pembekalan dan perkhidmatan; dan

c. memastikan jaminan daripada pembekal bahawa semua pembekalan dan perkhidmatan yang disediakan berfungsi dengan baik.

11.2 Pengurusan Penyampaian Perkhidmatan Pembekal

Objektif : Mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian di antara kerajaan dan pembekal.

11.2.1 Memantau dan Mengkaji Semula Perkhidmatan Pembekal

Peranan : ICTSO, Setiausaha Bahagian, Pembekal

KBS hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti berikut:

a. memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian;

b. menyemak laporan status kemajuan perkhidmatan oleh pembekal; dan

c. memaklumkan mengenai insiden keselamatan terhadap perkhidmatan kepada pembekal dan pemilik projek untuk tindakan sebagaimana perjanjian.

11.2.2 Menguruskan Perubahan Kepada Perkhidmatan Pembekal

Peranan : ICTSO, Setiausaha Bahagian, Pembekal

Sebarang perubahan kepada perkhidmatan hendaklah mengambil kira kepentingan maklumat, sistem dan *business process* yang terlibat serta melaksanakan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti berikut:

a. perubahan atau pengubahsuaian ke atas sesuatu sistem, polisi, prosedur dan lain-lain hendaklah bertujuan untuk meningkatkan dan menambahbaik perkhidmatan.

BIDANG 12: PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

12.1 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan

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

12.1.1 Tanggungjawab dan Prosedur

Peranan : ICTSO, CSIRT KBS

Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden KBS adalah berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT KBS yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut:

a. Memberikan kesedaran berkaitan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT KBS dan hebahan kepada warga KBS sekiranya ada perubahan; dan

b. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

12.1.2 Pelaporan Kejadian Keselamatan Maklumat

Peranan : ICTSO, Setiausaha/ Pengarah Bahagian, CSIRT KBS

a. Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT KBS. CSIRT KBS kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti berikut:

   i. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa;

ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;
iv. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan;
v. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
vi. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.

b. Prosedur pelaporan insiden keselamatan siber hendaklah mengikut pekeliling dan garis panduan sedia ada yang berkuatkuasa.

12.1.3 Pelaporan Kelemahan Keselamatan Maklumat

Peranan : Pengguna

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

12.1.4 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat

Peranan : ICTSO

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

12.1.5 Tindak Balas Terhadap Insiden Keselamatan Maklumat

Peranan : **ICTSO, CSIRT KBS**

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

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

i. mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;
ii. menjalankan kajian forensik sekiranya perlu;
iii. menghubungi pihak yang berkenaan 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.

12.1.6 Pembelajaran Daripada Insiden Keselamatan Maklumat

Peranan : ICTSO, CSIRT KBS

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

b. 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.

12.1.7 Pengumpulan Bahan Bukti

Peranan : ICTSO, CSIRT KBS

KBS hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.

.

BIDANG 13: ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

13.1 Kesinambungan Keselamatan Maklumat

Objektif : Memastikan kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan bisnes KBS.

13.1.1 Perancangan Kesinambungan Keselamatan Maklumat

Peranan : Jawatankuasa Pemandu PKP KBS

a. KBS hendaklah menentukan keperluan untuk keselamatan maklumat apabila berlaku kecemasan seperti krisis ekonomi, pendamik, bencana dan lain-lain;

b. KBS perlu merancang kesinambungan keselamatan maklumat dengan mengambil kira isu berkaitan yang boleh memberikan kesan ke atas perkhidmatan;

c. KBS juga perlu mengambil kira keperluan dan ekspektasi pihak berkepentingan dan peraturan semasa yang berkuatkuasa;

d. Perkara-perkara yang perlu diambilkira dalam merancang kesinambungan perkhidmatan adalah seperti berikut:

i. mengenalpasti maklumat yang perlu dilindungi mengikut tahap pengelasan yang telah ditetapkan;
ii. melaksanakan kajian impak perkhidmatan dan penilaian risiko terhadap perkhidmatan kritikal;
iii. membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan (BCP), Pelan Komunikasi Krisis (CCP), Pelan Tindak balas Kecemasan (ERP) dan Pelan Pemulihan Bencana ICT (DRP);
iv. melaksanakan program kesedaran dan latihan pasukan PKP serta warga KBS; dan
v. memastikan pelan ini disemak secara berjadual atau berdasarkan keperluan, dikemaskini dan diluluskan oleh pegawai yang bertanggungjawab.

13.1.2 Pelaksanaan Kesinambungan Keselamatan Maklumat

Peranan : Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT

KBS 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 berikut:

a. melaksanakan Pelan Kesinambungan Perkhidmatan (PKP) apabila berlaku terdapat gangguan terhadap perkhidmatan kritikal KBS dalam tempoh kecemasan;

b. melaksanakan *post-mortem* atau pasca-kejadian untuk mengenal pasti risiko baharu yang menjadi punca kegagalan perkhidmatan;

c. mengemas kini struktur tadbir urus PKP KBS jika berlaku pertukaran pegawai; dan

d. melaksanakan simulasi sekurang-kurangnya sekali setahun atau berdasarkan keperluan.

13.1.3 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat

Peranan : Jawatankuasa Pemandu PKP KBS

Mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.

Mengkaji semula, mengemaskini dan menilai PKP termasuk Pelan Pemulihan Bencana (*DRP*) sekurang-kurangnya sekali dalam setahun atau berdasarkan keperluan.

13.2 Lewahan (*Redundancy*)

Objektif : Mewujudkan lewahan sebagai sandaran untuk memastikan ketersediaan kemudahan pemprosesan maklumat dan perkhidmatan secara keseluruhan.

13.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat

Peranan : ICTSO, Pentadbir Sistem ICT, Pemilik Sistem

a. mewujudkan lewahan yang bersesuaian dan mencukupi bagi memastikan ketersediaan kemudahan pemprosesan maklumat secara berterusan; dan

b. lewahan perlu diuji keberkesanannya dari semasa ke semasa.

BIDANG 14: PEMATUHAN

14.1 Pematuhan Terhadap Keperluan Perundangan dan Kontrak

Objektif :  Meningkat dan memantapkan tahap keselamatan siber bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

14.1.1 Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai

Peranan : Pengguna

a. Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga KBS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KBS.

b. Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di KBS dan pembekal adalah seperti di **LAMPIRAN 2.**

14.1.2 Hak Harta Intelek

Peranan : Pengguna

a. Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual.

b. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.

14.1.3 Perlindungan Rekod

Peranan : Pengguna

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.

14.1.4 Privasi dan Perlindungan Maklumat Peribadi

Peranan: Pengguna

KBS hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.

14.1.5 Peraturan Kawalan Kriptografi

Peranan : Pengguna

KBS perlu memastikan kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan-peraturan. Perkara yang perlu dipatuhi adalah seperti berikut:

a. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi-fungsi kriptografi tanpa kelulusan pihak berkuasa;

b. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah/direka untuk mempunyai fungsi kriptografi tanpa kelulusan pihak berkuasa;

c. Sekatan penggunaan enkripsi yang tidak dibenarkan; dan

d. Mematuhi kaedah akses oleh pihak berkuasa Malaysia bagi maklumat enkripsi perkakasan dan perisian.

14.2 Kajian Semula Keselamatan Maklumat

Objektif : Memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur KBS.

14.2.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali

Peranan : ICTSO

Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.

14.2.2 Pematuhan Polisi dan Standard Keselamatan

Peranan : ICTSO

KBS hendaklah membuat kajian semula secara berkala terhadap pematuhan polisi dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.

14.2.3 Kajian Semula Pematuhan Teknikal

Peranan : ICTSO

KBS hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.

UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Pekeliling ICT KBS Bilangan 1 Tahun 2021 ini hendaklah dibaca bersama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuatkuasa antaranya seperti berikut:

1. Akta Hak Cipta (Pindaan) Tahun 1997;
2. Akta Jenayah Komputer 1997;
3. Akta Komunikasi dan Multimedia 1998;
4. Akta Rahsia Rasmi 1972;
5. Akta Tandatangan Digital 1997;
6. Akta Keselamatan Siber 2024.
7. Arahan Teknologi Maklumat 2007;
8. Arahan Keselamatan;
9. Arahan Perbendaharaan;
10. Pekeliling Am Bilangan 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
11. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- Agensi Kerajaan;
12. Pekeliling Perbendaharaan 5 Tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan (TPA);
13. Pekeliling Perkhidmatan Bil 5 2007 bertajuk Panduan Pengurusan Pejabat bertarikh 30 April 2007;
14. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan;
15. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 3 Tahun 2015 Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastruktur (GPKI)];
16. Pekeliling Transformasi Pentadbiran Awam Bil.3 Tahun 2017 Pengurusan Komunikasi Bersepadu Kerajaan (Government Unified Communication (1GovUC));

17. Pekeliling Kemajuan Pentadbiran Awam Bil.1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam;
18. Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam;
19. Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022;
20. Surat Pekeliling Am Bilangan 3 Tahun 2024 Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024;
21. Surat Pekeliling Am Bilangan 4 Tahun 2024 Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024;
22. Surat Arahan Ketua Pengarah MAMPU bertarikh 23 November 2007 Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan;
23. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
24. Perintah-Perintah Am;
25. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) April 2016;

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER KEMENTERIAN BELIA DAN SUKAN

NAMA (HURUF BESAR) :

NO. KAD PENGENALAN :

JAWATAN :

JABATAN / BAHAGIAN / AGENSI / SYARIKAT :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung dalam Polisi Keselamatan Siber Kementerian Belia dan Sukan; dan

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

TANDATANGAN :

TARIKH :

a) Pengesahan Ketua Pegawai Digital (CDO)

.....

( )