KPT.100-1/3/1 JLD2 (38)

KEMENTERIAN PENGAJIAN TINGGI

ARAHAN PENTADBIRAN KETUA SETIAUSAHA

BIL. 3 TAHUN 2021

POLISI KESELAMATAN SIBER
KEMENTERIAN PENGAJIAN TINGGI

TUJUAN

Arahan Pentadbiran ini bertujuan untuk menjelaskan mengenai Polisi Keselamatan Siber (PKS) Kementerian Pengajian Tinggi (KPT) yang perlu difahami dan dipatuhi oleh warga KPT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan teknologi maklumat dan komunikasi (ICT) KPT dalam melindungi aset ICT KPT.

LATAR BELAKANG

2. MAMPU telah mengeluarkan Surat Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan pada 1 Oktober 2000. Rangka Keselamatan ICT ini dirumus untuk memenuhi keperluan penguatkuasaan, kawalan dan langkah-langkah menyeluruh untuk melindungi aset ICT Kerajaan. Semua agensi Kerajaan dipertanggungjawabkan untuk memastikan Rangka Dasar Keselamatan ICT Kerajaan dilaksana dan dipatuhi.

3. Pada 9 Mac 2020, KPT diwujudkan semula dan dipisahkan daripada Kementerian Pendidikan Malaysia (KPM) selepas berlaku perubahan kepimpinan negara dan penstrukturan semula kementerian. Sehubungan dengan itu, Kementerian Pengajian Tinggi melalui Bahagian Pengurusan Maklumat telah menyediakan Polisi Keselamatan Siber (PKS) Versi 1.0 yang telah dibentang dan dipersetujui dalam Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KPT Bilangan 3 Tahun 2021 bertarikh 20 Mei 2021.

POLISI KESELAMATAN SIBER

4. Polisi Keselamatan Siber Versi 1.0 Kementerian Pengajian Tinggi seperti di **Lampiran A** adalah terpakai oleh semua pengguna termasuk kakitangan, pembekal, pakar runding dan pihak yang berurusan di Bahagian dan Agensi di bawah KPT yang mengurus, menyenggara, menyedia, memproses, mencapai, memuat turun, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT KPT.

TANGGUNGJAWAB BAHAGIAN DAN AGENSI DI BAWAH KPT

5. Semua Bahagian dan Agensi di bawah KPT adalah dikehendaki mematuhi Arahan Pentadbiran Ketua Setiausaha Bil. 3 Tahun 2021 Polisi Keselamatan Siber KPT dan melaksanakan tanggungjawab yang ditetapkan di dalamnya.

PEMAKAIAN

6. Arahan Pentadbiran ini dipanjangkan kepada semua Bahagian dan Agensi di bawah KPT kecuali Agensi Kelayakan Malaysia (MQA), Perbadanan Tabung Pendidikan Tinggi Nasional (PTPTN) dan Universiti Awam yang menggunakan aset ICT KPT. Polisi Keselamatan Siber KPT Versi 1.0 boleh dimuat turun melalui portal rasmi KPT https://www.mohe.gov.my.

TARIKH KUAT KUASA

7. Arahan Pentadbiran Ketua Setiausaha Bil. 3 Tahun 2021 ini berkuat kuasa mulai tarikh ia dikeluarkan.

PERTANYAAN

8. Sebarang pertanyaan mengenai polisi ini boleh dikemukakan kepada:

Setiausaha Bahagian
Bahagian Pengurusan Maklumat
Kementerian Pengajian Tinggi
Aras 6, No. 2, Menara 2
Jalan P5/6, Presint 5
62200 W.P. Putrajaya
No. Telefon : 03-8870 6060
E-mel : bpm.dasarict@mohe.gov.my

Sekian, terima kasih.

"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

(DATUK SERI DR. MAZLAN YUSOFF)
Ketua Setiausaha
Kementerian Pengajian Tinggi
29 Oktober 2021

Lampiran A

KEMENTERIAN PENGAJIAN TINGGI

POLISI KESELAMATAN SIBER

KEMENTERIAN PENGAJIAN TINGGI

Versi 1.0

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
20 Mei 2021	1.0	JPICT Bilangan 3 Tahun 2021	29 Oktober 2021

KANDUNGAN

TAKRIFAN

Bagi maksud pemakaian Pekeliling ICT KPT Bilangan 1 Tahun 2021 ini:

1.	Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
2.	Aset 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.	CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi.
11.	*Clear Desk* dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada 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.	*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).
20.	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
21.	*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.
22.	ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi.

23.	ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
24.	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
25.	Impak fungsi jabatan	Melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.
26.	Insiden keselamatan	Musibah (adverse event) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
27.	Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
28.	*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.
29.	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
30.	*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.
31.	*Intrusion Prevention System* (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau

		semua trafik rangkaian bagi sebarang kemungkinan serangan.
32.	ISDN	*Integrated Services Digital Network* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
33.	ISMS	*Information Security Management System* Sistem Pengurusan Keselamatan Maklumat.
34.	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
35.	KPT	Kementerian Pengajian Tinggi.
36.	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
37.	LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
38.	*Lock*	Mengunci komputer.
39.	*Logout*	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
40.	*Malicious Code*	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
41.	*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.

42.	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.
43.	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
44.	CERT KPT	Pasukan Tindakan Kecemasan/ *Computer Emergency Response* Team (CERT) KPT.
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 KPT, pembekal dan pihak-pihak lain yang diberi kebenaran menggunakan perkhidmatan ICT KPT.
47.	Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
48.	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.
49.	*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.
50.	*Rollback* (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.

51.	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.
52.	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
53.	*Server*	Pelayan komputer.
54.	*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.
55.	*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.
56.	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
57.	*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.
58.	*Video Conference*	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa yang sama ia diterima oleh penghantar.
59.	*Video Streaming*	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
60.	Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.

61.	WAN	*Wide Area Network.* Rangkaian yang merangkumi kawasan yang luas.
62.	Warga KPT	Kakitangan kerajaan yang berkhidmat di KPT, Bahagian, Jabatan dan agensi di bawahnya sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT KPT.
63.	*Wireless LAN*	Jaringan komputer yang terhubung tanpa melalui kabel.
64.	*Worm*	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

TUJUAN

1. Polisi Keselamatan Siber (PKS), Kementerian Pengajian Tinggi (KPT) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT dalam melindungi aset ICT KPT.

LATAR BELAKANG

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

OBJEKTIF

3. Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti berikut:

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

ii. Memastikan keselamatan penyampaian perkhidmatan KPT ditahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

iii. Memastikan kelancaran operasi KPT dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

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

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

ASET ICT KPT

4. Aset ICT KPT 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 KPT hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

a) Maklumat Rahsia Rasmi

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

b) Maklumat Rasmi

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

d) Data Terbuka

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

ii. Aliran Data

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

a) Saluran komunikasi dan aliran data antara sistem di KPT;
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 (Closed-Circuit Television System (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 KPT yang dihubungkan dengan sistem KPT. 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 KPT. 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 KESELAMATAN ICT

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

6. Penilaian risiko keselamatan ICT hendaklah dilaksanakan secara berkala atau apabila berlaku sebarang perubahan kepada persekitaran ruang siber KPT.

7. 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

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

iii. Impak

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

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 KPT 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

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

i. Prinsip "Perlu-Tahu"

KPT 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), KPT hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

iv. Kawalan Capaian Berdasarkan Peranan

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

v. Peminimuman Data

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

TEKNOLOGI

9. 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

1) KPT 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

KPT 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

1) KPT 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 KPT 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, KPT hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (counter measure dan control measure) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

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

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

a) Peranti Pengkomputeran Peribadi

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

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

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 manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah 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. Pelayan hendaklah 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) KPT hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

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) MAMPU 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) KPT hendaklah merujuk kepada MAMPU untuk mendapatkan nasihat mengenai perkhidmatan pengkomputeran awan yang akan dilaksanakan dan mematuhi polisi yang digariskan.

PROSES

10. KPT hendaklah melindungi keselamatan ICT dengan melaksanakan perkara-perkara berikut:

i. Konfigurasi Asas

a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan.

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 untuk memastikan bahawa proses kerja boleh dilaksanakan.

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 KPT 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

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

12. 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 KPT.

i. Kompetensi Pengguna

a) Kompetensi pengguna termasuk:

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

2) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga KPT 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 KPT 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 ICT; dan
4) Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

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

iii. Peranan Penguna

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

b) Setiap orang 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 KPT yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Kementerian dikembalikan sekiranya berlaku perubahan peranan.

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

f) Warga KPT lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Kementerian dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Kementerian.

PERNYATAAN POLISI KESELAMATAN SIBER KPT

13. 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.

14. 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.

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

16. Sebanyak 14 bidang keselamatan yang terlibat di dalam Polisi Keselamatan Siber KPT diterangkan dengan lebih jelas dan teratur seperti berikut:

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 KPT dan perundangan yang berkaitan.

1.1.1 Polisi Keselamatan Maklumat

Peranan	Keterangan
▪ KSU ▪ CIO ▪ ICTSO ▪ JPICT ▪ Setiausaha/ Pengarah Bahagian	Pelaksanaan polisi ini akan dijalankan oleh Ketua Setiausaha (KSU) KPT dengan disokong oleh Jawatankuasa Pemandu ICT (JPICT) yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan ahli-ahli yang dilantik oleh KSU KPT. Polisi Keselamatan Siber (PKS) KPT mestilah dipatuhi oleh semua warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan KPT kepada warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT.

1.1.2 Kajian Semula Polisi untuk Keselamatan Maklumat

Peranan	Keterangan
▪ CIO ▪ 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 KPT: a. Mengenal pasti dan menentukan perubahan yang diperlukan; b. Mengemukakan cadangan pindaan untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan;

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

2.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat

Peranan	Tanggungjawab
Ketua Setiausaha	a. Memastikan penguatkuasaan pelaksanaan Polisi ini; b. Memastikan warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; c. Memastikan semua keperluan KPT seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi; d. Memastikan pengurusan risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan e. Melantik CIO dan ICTSO.
Ketua Pegawai Maklumat (CIO)	a. Membantu Ketua Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT seperti yang ditetapkan di dalam Polisi ini; b. Memastikan kawalan keselamatan maklumat dalam KPT diseragam dan diselaraskan dengan sebaiknya; c. Memastikan Pelan Strategik Pendigitalan KPT mengandungi aspek keselamatan ICT; dan d. Menyelaras pelan latihan dan program kesedaran keselamatan ICT.

Peranan	Tanggungjawab
Pegawai Keselamatan ICT (ICTSO)	a. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; b. Merangka pengurusan risiko dan audit keselamatan ICT berpandukan rangka kerja, polisi dan pekeliling/garis panduan yang berkuat kuasa; c. Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan ICT dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; d. Melaporkan insiden keselamatan ICT kepada CERT KPT dan seterusnya membantu dalam penyiasatan atau pemulihan; e. Melaporkan insiden keselamatan ICT kepada CIO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP); f. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; g. Melaksanakan pematuhan Polisi ini oleh warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT; h. Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT; dan i. Menyedia dan merangka latihan dan program kesedaran keselamatan ICT.
Setiausaha/ Pengarah Bahagian	a. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu;

Peranan	Tanggungjawab
	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.
Pentadbir Sistem ICT	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 di dalam Polisi ini; c. Memantau aktiviti capaian sistem aplikasi; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; e. Menganalisis dan menyimpan rekod jejak audit; dan f. Menyediakan laporan mengenai aktiviti capaian secara berkala.
Pentadbir Rangkaian	Pentadbir Rangkaian ICT berperanan menguruskan rangkaian di KPT.
Jawatankuasa Pemandu ICT (JPICT)	Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil. 3 Tahun 2015 ialah merancang dan menentukan langkah-langkah keselamatan ICT.

Peranan	Tanggungjawab
Computer Emergency Response Team (CERT) KPT	a. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b. Merekod dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d. Menasihati Pentadbir Sistem/pelayan untuk mengambil tindakan pemulihan dan pengukuhan; dan e. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Pentadbir Sistem ICT.
Pengguna/ Warga KPT	a. Membaca, memahami dan mematuhi Polisi ini; b. Mengetahui dan memahami implikasi keselamatan ICT 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 ICT yang ditetapkan; vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan,

Peranan	Tanggungjawab
	pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan kawalan keselamatan ICT dari diketahui umum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada CERT KPT dengan segera; g. Menghadiri program-program kesedaran mengenai keselamatan ICT; h. Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini; dan i. Menandatangani **Surat Akuan Pematuhan PKS KPT (LAMPIRAN 2)**;
Bahagian Pengurusan Maklumat (BPM)	Membangun serta menyebarkan polisi dan langkah-langkah keselamatan ICT kepada Warga KPT.

2.1.2 Pengasingan Tugas

Peranan	Keterangan
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;

Peranan	Keterangan
	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	Keterangan
▪ CERT KPT	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 KPT; 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	Keterangan
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	Keterangan
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 KPT; 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 KPT; dan

Peranan	Keterangan
	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	Keterangan
Bahagian Pengurusan Maklumat (BPM)	Membangun serta menyebarkan polisi dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul berkaitan penggunaan peranti mudah alih.
Jawatankuasa Pemandu ICT (JPICT)	Meluluskan polisi, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga KPT.
Warga KPT	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

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

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

2.2.3 Mesyuarat Dalam Talian

Peranan	Keterangan
Penyelaras/ Pentadbir Mesyuarat	Mesyuarat dalam talian hendaklah mengadaptasi teknik yang selamat seperti penggunaan kata laluan sebelum dibenarkan terlibat di dalam mesyuarat berkenaan.
Warga KPT	Polisi dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, dibincang atau disimpan semasa mesyuarat dalam talian.

BIDANG 03 :
KESELAMATAN SUMBER MANUSIA

3.1 Sebelum Perkhidmatan

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

3.1.1 Tapisan Keselamatan

Peranan	Keterangan
▪ Pengguna	Tapisan keselamatan hendaklah dijalankan terhadap warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b. Menjalankan tapisan keselamatan untuk warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT 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	Keterangan
▪ Pengguna	Persetujuan berkontrak dengan warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

Peranan	Keterangan
	a. Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT 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 KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT 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	Keterangan
▪ Pengguna	Pengurusan hendaklah memastikan warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.

3.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat

Peranan	Keterangan
▪ Pengguna	Warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT 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 KPT, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan

Peranan	Keterangan
	dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; b. Memastikan kesedaran yang berkaitan PKS KPT 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	Keterangan
▪ Setiausaha/ Pengarah Bahagian	Proses tatatertib yang formal dan disampaikan kepada warga KPT hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga KPT 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 KPT sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh KPT; dan b. Warga KPT yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT KPT.

3.3 Penamatan dan Pertukaran Perkhidmatan

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

3.3.1 Penamatan atau Pertukaran Tanggung Jawab Perkhidmatan

Peranan	Keterangan
▪ Warga KPT	Warga KPT yang telah tamat perkhidmatan hendaklah: a. Memastikan semua aset ICT dikembalikan kepada KPT 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 KPT dan/atau terma perkhidmatan yang ditetapkan; dan c. Maklumat rasmi KPT dalam peranti tidak dibenarkan dibawa keluar dari KPT. Warga KPT yang telah bertukar perkhidmatan hendaklah: a. Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada KPT 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 KPT.

4.1.1 Inventori Aset

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pegawai Aset ▪ Pengguna	Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT KPT. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a. KPT 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	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pengguna	Aset yang diselanggara hendaklah hak milik KPT. 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;

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

4.1.4 Pemulangan Aset

Peranan	Keterangan
Pengguna	Warga KPT hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan 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	Keterangan
Pegawai Pengelas	Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.

4.2.2 Pelabelan Maklumat

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

4.2.3 Pengendalian Aset

Peranan	Keterangan
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 ICT 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	Keterangan
▪ Pentadbir Sistem ICT ▪ Pengguna	Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh KPT. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:

Peranan	Keterangan
	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	Keterangan
▪ 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	Keterangan
▪ 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	Keterangan
▪ CIO ▪ ICTSO ▪ 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	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Rangkaian	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 KPT, 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 Pembatalan Pengguna

Peranan	Keterangan
▪ Pengguna	Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara–perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh KPT sahaja boleh digunakan; b. Akaun pengguna mestilah unik; c. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada KPT terlebih dahulu;

Peranan	Keterangan
	d. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan KPT.

5.2.2 Peruntukan Akses Pengguna

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT	Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.

5.2.3 Pengurusan Hak Akses Istimewa

Peranan	Keterangan
▪ Pentadbir Sistem ICT	a. Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan 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	Keterangan
▪ ICTSO ▪ 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	Keterangan
▪ ICTSO ▪ 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	Keterangan
▪ 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 KPT.

5.3 Tanggungjawab Pengguna

Objektif : Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.

5.3.1 Penggunaan Maklumat Pengesahan Rahsia

Peranan	Tanggungjawab
▪ Setiausaha/ Pengarah Bahagian ▪ ICTSO ▪ Pentadbir Sistem ICT ▪ Pengguna	a. Membaca, memahami dan mematuhi PKS KPT; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat KPT; 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;

Peranan	Tanggungjawab
	iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum. e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan f. Menghadiri program-program kesedaran mengenai keselamatan ICT.

5.3.2 Penggunaan Maklumat Pengesahan Rahsia

Peranan	Keterangan
▪ Pentadbir Sistem ▪ Pengguna	Pengguna perlu 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	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ▪ Pengguna	Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut polisi kawalan capaian.

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

Peranan	Keterangan
▪ Pentadbir Sistem	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 KPT; 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	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ ICTSO ▪ Pentadbir Sistem ▪ Pengguna	Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KPT seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

Peranan	Keterangan
	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 hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; g. Kuat kuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan; 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	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT	Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.

5.4.5 Kawalan Akses Kepada Kod Sumber Program

Peranan	Keterangan
▪ Pentadbir Sistem ICT ▪ Pemilik Sistem ▪ 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 KPT.

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	Keterangan
▪ 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	Keterangan
▪ Pentadbir sistem ▪ Pengguna	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.

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 KPT.

7.1.1 Perimeter Keselamatan Fizikal

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian	Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT KPT. Perkara-perkara yang perlu dipatuhi seperti berikut: a. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; b. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; c. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; d. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; e. Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; f. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal

Peranan	Keterangan
	dari pihak yang tidak diberi kebenaran memasukinya; dan g. Memasang alat penggera atau kamera keselamatan.

7.1.2 Kawalan Kemasukan Fizikal

Peranan	Keterangan
▪ Pengguna	Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis KPT. Perkara yang perlu dipatuhi adalah seperti berikut: a. Warga KPT hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada KPT apabila bertukar, tamat perkhidmatan atau bersara; b. Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; c. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT KPT; dan d. Kehilangan pas keselamatan hendaklah dilaporkan segera kepada Pihak Berkuasa.

7.1.3 Keselamatan Pejabat, Bilik dan Kemudahan

Peranan	Keterangan
▪ 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 *Closed-Circuit Television* (CCTV) dan pusat data perlu dihadkan daripada diakses tanpa kebenaran;

Peranan	Keterangan
	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.

7.1.4 Perlindungan Daripada Ancaman Luar Dan Persekitaran

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Bahagian Khidmat Pengurusan (BKP)	Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. KPT perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.

7.1.5 Bekerja di Kawasan Selamat

Peranan	Keterangan
▪ 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 KPT yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis KPT 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;

Peranan	Keterangan
	ii. Akses adalah terhad kepada warga KPT yang telah diberi kuasa sahaja dan dipantau pada setiap masa; iii. Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai; iv. Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; v. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; vi. Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; vii. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; viii. Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; ix. Memperkukuh dinding dan siling; dan x. Mengehadkan jalan keluar masuk.

7.1.6 Kawasan Penyerahan dan Pemunggahan

Peranan	Keterangan
▪ 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. KPT 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 KPT daripada kehilangan, kerosakan, kecurian dan disalahgunakan.

7.2.1 Penempatan dan Perlindungan Peralatan ICT

Peranan	Keterangan
▪ Pengguna	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. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; e. Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; f. Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna; g. Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; h. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set);

Peranan	Keterangan
	i. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; j. Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci; k. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; l. Peralatan ICT yang hendak dibawa ke luar premis KPT, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; m. Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; n. Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT; p. Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; q. Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r. Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; s. Pengguna dilarang sama sekali mengubah ***password administrator*** yang telah ditetapkan oleh pihak ICT; dan

Peranan	Keterangan
	t. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan KPT sahaja.

7.2.2 Utiliti Sokongan

Peranan	Keterangan
▪ Pengguna	a. Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan; dan b. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).

7.2.3 Keselamatan Kabel

Peranan	Keterangan
▪ 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

Peranan	Keterangan
	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	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT	a. Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. b. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. c. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: i. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; ii. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; iii. Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; iv. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan v. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

7.2.5 Pengalihan Aset

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT	Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a. Peralatan ICT yang hendak dibawa keluar dari premis KPT untuk tujuan rasmi, perlulah mendapat kelulusan KSU atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.

7.2.6 Keselamatan Peralatan dan Aset di Luar Premis

Peranan	Keterangan
▪ Pengguna	Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis KPT. Peralatan yang dibawa keluar dari premis KPT 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.

7.2.7 Pelupusan yang Selamat atau Penggunaan Semula Peralatan

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT ▪ Pegwai Aset ▪ Pengguna	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 KPT dan ditempatkan di KPT. 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 KPT. Langkah-langkah seperti berikut hendaklah diambil: i. Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat; ii. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; iii. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; iv. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; v. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: 1. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; 2. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *Central*

Peranan	Keterangan
	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 KPT; 4. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan 5. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab KPT. d. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumbdrive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; e. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan; f. Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa; g. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan h. Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori MyAsset.

7.2.8 Peralatan Pengguna Tanpa Kawalan

Peranan	Keterangan
▪ Pengguna	a. Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya; dan b. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: i. Tamatkan sesi aktif apabila selesai tugas; ii. *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan iii. Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.

7.2.9 Polisi Meja Kosong dan Skrin Kosong

Peranan	Keterangan
▪ Pengguna	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* 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; 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

Peranan	Keterangan
	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	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT	Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut: a. Semua prosedur keselamatan ICT 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	Keterangan
▪ Pentadbir Sistem ICT	Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;

Peranan	Keterangan
	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	Keterangan
▪ Pemilik Sistem ▪ Pentadbir Sistem	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 ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

8.1.4 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi

Peranan	Keterangan
▪ Pentadbir Sistem ICT	Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian

Peranan	Keterangan
	yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (production); b. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan c. Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

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	Keterangan
▪ Pentadbir Sistem 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;

Peranan	Keterangan
	c. Mengimbas semua perisian atau sistem 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 Sandaran

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

8.3.1 Sandaran Maklumat

Peranan	Keterangan
▪ Pentadbir Sistem ICT	a. Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui; dan b. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off site*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

Peranan	Keterangan
	i. Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; ii. Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi; iii. Menguji sistem sandaran sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan iv. Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara **harian, mingguan, bulanan** atau **tahunan**. Kekerapan sandaran 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	Keterangan
▪ Pentadbir Sistem 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.

Peranan	Keterangan
	e. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: i. Fail log sistem pengoperasian; ii. Fail log servis (contoh: *web*, e-mel); iii. Fail log aplikasi (audit trail); dan iv. Fail log rangkaian (contoh: *switch, firewall*). f. Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: i. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; ii. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan iii. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada CERT KPT.

8.4.2 Perlindungan Maklumat Log

Peranan	Keterangan
▪ Pentadbir Sistem ICT	Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.

8.4.3 Log pentadbir dan Pengendali

Peranan	Keterangan
▪ Pentadbir Sistem ▪ CERT KPT	Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap seperti berikut: a. Memantau penggunaan kemudahan memproses maklumat secara berkala; b. Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu; c. Kesalahan, kesilapan dan/ atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; d. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan e. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada CERT KPT.

8.4.4 Penyeragaman Jam

Peranan	Keterangan
▪ Pentadbir Pusat Data	a. Aktiviti jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal; dan b. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KPT atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *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	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT	Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti berikut: a. Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; b. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan c. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

8.6 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	Keterangan
▪ Pentadbir Sistem ICT ▪ CERT KPT	Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:

Peranan	Keterangan
	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	Keterangan
▪ Pentadbir sistem 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 warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT. 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	Keterangan
▪ ICTSO ▪ Pentadbir Sistem ICT	Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perkhidmatann di KPT.

BIDANG 09 :
KESELAMATAN KOMUNIKASI

9.1 Pengurusan Keselamatan Rangkaian

Objektif : Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

9.1.1 Kawalan Rangkaian

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ ICTSO ▪ Pentadbir Rangkaian	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 KPT; 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

Peranan	Keterangan
	aktiviti-aktiviti lain yang boleh mengancam data dan maklumat KPT; i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan BPM, KPT adalah tidak dibenarkan; k. Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di KPT sahaja dan penggunaan MODEM adalah dilarang sama sekali; l. Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya; m. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; n. Menempatkan atau memasang antara muka (interfaces) yang bersesuaian di antara rangkaian KPT, rangkaian agensi lain dan rangkaian awam; o. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; p. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; q. Mengawal capaian fizikal dan logikal ke atas kemudahan *port* diagnostik dan konfigurasi jarak jauh; r. Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan KPT; dan s. Mewujud dan melaksana kawalan pengalihan laluan (routing control) bagi memastikan pematuhan terhadap peraturan KPT.

9.1.2 Keselamatan Perkhidmatan Rangkaian

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Rangkaian ▪ 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	Keterangan
▪ Pentadbir Rangkaian	Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian KPT.

9.2 Pemindahan Data dan Maklumat

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

9.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat

Peranan	Keterangan
▪ Pengguna	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 KPT dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; c. Media yang mengandungi maklumat perlu dilindungi; dan d. Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.

9.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat

Peranan	Keterangan
▪ CIO ▪ Setiausaha/ Pengarah Bahagian	KPT perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara KPT dengan pihak luar. Perkara yang perlu dipertimbangkan ialah: a. Setiausaha/Pengarah Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat KPT; b. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat KPT; c. Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan d. KPT hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan dan data dalam simpanan bagi menghalang ketirisan data.

9.2.3 Pesanan Elektronik

Peranan	Keterangan
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 adalah seperti **LAMPIRAN 1**: a. Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003; b. Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 – Pematuhan Tatacara Penggunaan E-mel dan Internet;

Peranan	Keterangan
	c. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkah-langkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan; d. Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication* (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa; dan e. Sebarang e-mel rasmi hendaklah direkod ke dalam DDMS 2.0 untuk tujuan rekod.

9.2.4 Perjanjian Kerahsiaan atau Ketakdedahan

Peranan	Keterangan
▪ ICTSO ▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT ▪ Pengguna	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 yang relevan.

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	Keterangan
▪ Pentadbir Sistem ICT	Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah 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 KPT; 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

Peranan	Keterangan
▪ Pentadbir Sistem 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 KPT; 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

Peranan	Keterangan
▪ ICTSO ▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT	Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;

Peranan	Keterangan
	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

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

10.2.1 Polisi Pembangunan Selamat

Peranan	Keterangan
▪ ICTSO ▪ Setiausaha/ Pengarah Bahagian ▪ 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

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem 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

Peranan	Keterangan
	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 d. Capaian kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.

10.2.3 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi

Peranan	Keterangan
▪ Pentadbir Sistem 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

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem 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

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem 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

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem 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. KPT perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: i. Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; ii. Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; iii. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; iv. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; v. Pegawai yang bekerja di dalam persekitaran pembangunan sistem ~~ialah yang~~ boleh dipercayai; dan vi. Kawalan ke atas capaian kepada persekitaran pembangunan sistem.

10.2.7 Pembangunan oleh Khidmat Luaran

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ ICTSO	KPT hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (source code) adalah menjadi

Peranan	Keterangan
▪ Pentadbir Sistem ICT	**HAK MILIK** KPT. Perkara yang perlu dipatuhi adalah seperti berikut: a. Perkiraan perlesenan, kod sumber ialah **HAK MILIK** KPT 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

Peranan	Keterangan
▪ ICTSO ▪ Pentadbir Sistem 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; dan

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

10.2.9 Pengujian Penerimaan Sistem

Peranan	Keterangan
▪ ICTSO ▪ 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); b. Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan c. Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (vulnerability scanner).

10.3 Data Ujian

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

10.3.1 Perlindungan Data Ujian

Peranan	Keterangan
▪ 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;

Peranan	Keterangan
	b. Personel 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 KPT yang boleh dicapai oleh pembekal dilindungi.

11.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pembekal	Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset KPT. 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 KPT (LAMPIRAN 3)**.

11.1.2 Menangani Keselamatan Dalam Perjanjian Pembekal

Peranan	Keterangan
▪ Syarikat 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. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak KPT selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa; c. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: i. KPT hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; ii. Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; iii. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; iv. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; v. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;

Peranan	Keterangan
	vi. Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: 1) Badan penilai pihak ketiga adalah bebas dan berintegriti; 2) Badan penilai pihak ketiga adalah kompeten; 3) Kriteria penilaian; 4) Parameter pengujian; 5) Andaian yang dibuat berkaitan dengan skop penilaian; vii. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan KPT; dan viii. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh KPT.

11.1.3 Rantaian Bekalan Teknologi Maklumat dan Komunikasi

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pembekal	Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan ICT serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan c. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.

11.2 Pengurusan Penyampaian Perkhidmatan Pembekal

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

11.2.1 Memantau dan Mengkaji Semula Perkhidmatan Pembekal

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pembekal	KPT 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 perkhidmatan; b. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan c. Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.

11.2.2 Menguruskan Perubahan Kepada Perkhidmatan Pembekal

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pembekal	Perubahan kepada peruntukan perkhidmatan oleh pembekal termasuk mempertahan dan menambah baik polisi keselamatan maklumat sedia ada, prosedur dan kawalan hendaklah diuruskan dengan mengambil kira kepentingan maklumat, sistem dan proses bisnes yang terlibat serta penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti berikut: a. Perubahan dalam perjanjian dengan pembekal; b. Perubahan yang dilakukan oleh KPT bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian polisi dan prosedur; dan

Peranan	Keterangan
	c. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.

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	Keterangan
▪ ICTSO ▪ CERT KPT	Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden KPT adalah berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CERT KPT yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memberikan kesedaran berkaitan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CERT KPT dan hebahan kepada warga KPT sekiranya ada perubahan; dan b. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

12.1.2 Pelaporan Kejadian Keselamatan Maklumat

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ ICTSO ▪ CERT KPT	a. Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada CERT KPT. CERT KPT 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;

Peranan	Keterangan
	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 ICT berdasarkan: i. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; ii. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan iii. Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT.

12.1.3 Pelaporan Kelemahan Keselamatan Maklumat

Peranan	Keterangan
▪ Pengguna	Warga KPT dan pembekal yang menggunakan sistem dan perkhidmatan maklumat KPT dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.

12.1.4 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat

Peranan	Keterangan
▪ 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	Keterangan
▪ ICTSO ▪ CERT KPT	**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	Keterangan
▪ ICTSO ▪ CERT KPT	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	Keterangan
▪ ICTSO ▪ CERT KPT	KPT 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 KPT.

13.1.1 Perancangan Kesinambungan Keselamatan Maklumat

Peranan	Keterangan
▪ ICTSO ▪ CERT KPT ▪ Pentadbir Sistem ICT	a. KPT hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana; b. Dalam merancang kesinambungan keselamatan maklumat, KPT perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi KPT; c. KPT juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti berikut: i. Membangunkan Pelan Kesinambungan Perkhidmatan dengan mengenal pasti aspek keselamatan maklumat yang terlibat; ii. Mengenal pasti keselamatan maklumat pada lokasi dan Pelan Kesinambungan Perkhidmatan; iii. Memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan KPT; dan iv. Memastikan pelan ini diluluskan oleh pegawai yang bertanggungjawab.

13.1.2 Pelaksanaan Kesinambungan Keselamatan Maklumat

Peranan	Keterangan
▪ ICTSO ▪ CERT KPT ▪ Pentadbir Sistem ICT	KPT 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 PKP apabila terdapat gangguan terhadap perkhidmatan kritikal KPT yang telah dikenal pasti berdasarkan kepada Pelan Pengurusan Kesinambungan Perkhidmatan dan Pelan Pemulihan Bencana ICT terkini; b. Melaksanakan *post-mortem* dan mengemaskini pelan-pelan PKP; c. Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal KPT; d. Mengemas kini struktur tadbir urus PKP KPT jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan e. Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.

13.1.3 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat

Peranan	Keterangan
▪ Pengurusan Atasan KPT ▪ CERT KPT	KPT hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.

13.2 Lewahan

Objektif : Memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.

13.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian ▪ Pentadbir Sistem ICT	Kemudahan pemprosesan maklumat KPT perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (failover test) keberkesanannya dari semasa ke semasa.

BIDANG 14:
PEMATUHAN

14.1 Pematuhan Terhadap Keperluan Perundangan dan Kontrak

Objektif : Meningkat dan memantapkan tahap keselamatan ICT 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	Keterangan
▪ Pengguna	a. Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT. b. Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di KPT dan pembekal adalah seperti di **LAMPIRAN 2.**

14.1.2 Hak Harta Intelek

Peranan	Keterangan
▪ 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	Keterangan
▪ 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	Keterangan
▪ Pengguna	KPT 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	Keterangan
▪ Pengguna	KPT 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 KPT.

14.2.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali

Peranan	Keterangan
▪ Setiausaha/ Pengarah Bahagian	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	Keterangan
▪ Setiausaha/ Pengarah Bahagian	KPT 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	Keterangan
▪ Setiausaha/ Pengarah Bahagian	KPT hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.

LAMPIRAN 1

UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Pekeliling ICT KPT 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 Rahsia Rasmi 1972;

2. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama) - "Tatacara Penyediaan, Penilaian dan PenerimaanTender";

3. Surat Pekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan";

4. Akta Tandatangan Digital 1997;

5. Akta Jenayah Komputer 1997;

6. Akta Hak Cipta (Pindaan) Tahun 1997;

7. Akta Komunikasi dan Multimedia 1998;

8. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";

9. Surat Akujanji (Pekeliling Perkhidmatan Bilangan 17 Tahun 2001);

10. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

11. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002;

12. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";

13. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

14. Surat Pekeliling Am Bil. 4 Tahun 2006 – "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";

15. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk “Tatacara Pengurusan Aset Alih Kerajaan (TPA)”;

16. Pekeliling Perkhidmatan Bil 5 2007 bertajuk “Panduan Pengurusan Pejabat” bertarikh 30 April 2007;

17. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 “Langkah-langkah mengenai penggunaan Mel Elektronik Agensi – Agensi Kerajaan”, Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC);

18. Arahan Teknologi Maklumat 2007;

19. Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk “Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan”;

20. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk “Penggunaan Media Jaringan Sosial di Sektor Awam”;

21. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam;

22. Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 bertajuk “Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)]” bertarikh 23 Oktober 2015;

23. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;

24. Arahan Keselamatan (Semakan dan Pindaan 2017);

25. Myportfolio (Pekeliling Kemajuan Pentadbiran Awam Bil 4 Tahun 2018);

26. Pekeliling Perkhidmatan Bilangan 5 Tahun 2020. Dasar Bekerja Dari Rumah;

27. Arahan Pentadbiran Ketua Pengarah MAMPU Bilangan 4 Tahun 2020 - Polisi Keselamatan Siber MAMPU;

28. Surat edaran arahan dalaman KPT.500-7/3/1(82) bertarikh 31 Mei 2021 berkaitan Pematuhan Mesyuarat Atas Talian;

29. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2001 bertajuk “Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam” bertarikh 10 Jun 2021;

30. Perintah-Perintah Am;

31. Arahan Perbendaharaan;

LAMPIRAN 2

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER KEMENTERIAN PENGAJIAN TINGGI

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
( )
b.p. Ketua Setiausaha KPT
Tarikh :

LAMPIRAN 3

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER KEMENTERIAN PENGAJIAN TINGGI

Nama (Huruf Besar) .....

No. Kad Pengenalan .....

Jawatan .....

Syarikat .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

3. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub di dalam Polisi Keselamatan Siber KPT; dan

4. Sekiranya saya atau mana-mana individu yang mewakili syarikat ini didapati melanggar polisi yang telah ditetapkan, maka saya sebagai wakil syarikat bersetuju tindakan undang-undang boleh diambil ke atas sesiapa yang terlibat mengikut peruntukan undang-undang sedia ada yang sedang berkuatkuasa.

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
( )
b.p. Ketua Setiausaha KPT
Tarikh :