KEMENTERIAN SAINS,
TEKNOLOGI DAN INOVASI

POLISI KESELAMATAN SIBER

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI

MERAKYATKAN SAINS
MENGINSANKAN TEKNOLOGI
MENGARUSPERDANAKAN INOVASI

MALAYSIA MADANI

KEMENTERIAN SAINS,
TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

POLISI KESELAMATAN SIBER

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI

PKS MOSTI Versi 2.0
Diterbitkan Pada 4 April 2024

ISI KANDUNGAN

TERMA DAN DEFINISI

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dasar ini:

Bil.	Istilah	Penerangan
(1)	*Active Directory* AD	Teknologi yang dikeluarkan oleh pihak Microsoft yang digunakan untuk mengurus maklumat akaun pengguna di dalam satu direktori.
(2)	Agensi Luar	Organisasi Kerajaan atau swasta yang berurusan dengan Kementerian.
(3)	Akaun Pengguna	Akaun yang membolehkan pengguna mencapai sistem aplikasi seperti e-mel, intranet dan lain-lain.
(4)	*Antivirus*	Perisian yang digunakan untuk mengesan dan menghapuskan virus komputer pada komputer atau sebarang media storan mudah alih seperti *thumb drive, external drive* dan lain-lain.
(5)	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.
(6)	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
(7)	*Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
(8)	Bahagian/Unit	Bahagian/Unit di bawah Kementerian.
(9)	Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
(10)	*Bandwidth*	Jalur lebar. Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
(11)	BPTM	Bahagian Pengurusan Teknologi Maklumat.
(12)	BT	Bahagian Pentadbiran. Bahagian yang bertanggungjawab menyediakan perkhidmatan infrastruktur kerja, keselamatan, penyelenggaraan persekitaran kerja dan perkhidmatan lain yang berkaitan di Kementerian.

Bil.	Istilah	Penerangan
(13)	*BYOD*	*Bring Your Own Device.* Peralatan seperti komputer riba, *ipad* dan peralatan lain kepunyaan persendirian untuk digunakan di pejabat.
(14)	CCT	*Crisis Communication Team.* Pasukan Komunikasi Krisis.
(15)	CCTV	*Closed-Circuit Television System.* Sistem TV yang digunakan secara komersit di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
(16)	CDO	*Chief Digital Officer.* Ketua Pegawai Digital bagi MOSTI ialah Setiausaha Bahagian Kanan (Pengurusan) yang bertanggungjawab terhadap budaya kerja yang dipacu oleh teknologi digital.
(17)	CIA	*Confidentiality, Integrity, Availability.*
(18)	*Clear Desk and 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.
(19)	COTS	*Commercial Off-The-Shelf.* Produk perisian atau peralatan komersial yang telah siap dan sedia untuk digunakan sama ada dengan membelinya, disewa ataupun dilesenkan.
(20)	CSIRT Kementerian	Pasukan Tindak Balas Insiden Keselamatan Siber (*Cyber Security Incident Response Team,* CSIRT) Kementerian yang terdiri daripada pegawai yang bertanggungjawab menjaga keselamatan ICT di Ibu Pejabat dan Jabatan/Agensi di bawah MOSTI.
(21)	*Data-at-rest*	Data Dalam Simpanan. Merujuk kepada data yang disimpan di lokasi sistem yang kukuh dan stabil. Data Dalam Simpanan ialah data yang tidak lagi digunakan atau dipindahkan ke lain-lain lokasi.
(22)	*Data-in-motion*	Data Dalam Pergerakan. Merujuk kepada data yang sedang bergerak menuju ke sesuatu lokasi atau dipindahkan melalui sistem rangkaian.

Bil.	Istilah	Penerangan
(23)	*Data-in-use*	Data Dalam Penggunaan. Merujuk kepada data yang sedang digunakan atau beroperasi. Kedudukan Data Dalam Penggunaan bukan secara pasif di lokasi tertentu yang stabil. Data ini berfungsi di dalam arkitektur teknologi maklumat.
(24)	*Denial of service*	Gangguan ke atas perkhidmatan yang menyebabkan kegagalan capaian kepada perkhidmatan. Ia juga dikenali sebagai penafian perkhidmatan.
(25)	*Defence-in-depth*	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
(26)	DRT	*Disaster Recovery Team.* Pasukan Pemulihan Bencana.
(27)	DRMP	*Disaster Recovery Management Plan*
(28)	DRTP	*Disaster Recovery Technical Plan*
(29)	ERT	*Emergency Response Team.* Pasukan Tindak Balas Kecemasan.
(30)	*Escrow*	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
(31)	*Firewall*	Sistem pertahanan yang melindungi infrastruktur ICT dari pelbagai ancaman luaran dan dalaman.
(32)	*Hard disk*	Cakera Keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
(33)	*Hub*	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan *(broadcast)* data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
(34)	ICT	*Information and Communication Technology.* Teknologi Maklumat dan Komunikasi.
(35)	ICTSO	*ICT Security Officer.* Pegawai Keselamatan ICT bagi Kementerian ialah Setiausaha Bahagian BPTM di Kementerian yang bertanggungjawab terhadap keselamatan sistem komputer.

Bil.	Istilah	Penerangan
(36)	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
(37)	Impak fungsi jabatan	Melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.
(38)	Insiden Keselamatan	Musibah *(adverse event)* yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
(39)	*Internet*	Sistem rangkaian seturuh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
(40)	*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.
(41)	*Intranet*	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
(42)	IPS	*Intrusion Prevention System.* 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.
(43)	IDS	*Intrusion Detection System.* 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.
(44)	ISDN	*Integrated Services Digital Network.* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
(45)	ISMS	*Information Security Management System.* Sistem Pengurusan Keselamatan Maklumat.

Bil.	Istilah	Penerangan
(46)	Jabatan/Agensi Kementerian	Agensi Kerajaan di bawah seliaan Kementerian.
(47)	JDN	Jabatan Digital Negara
(48)	JKICT	Jawatankuasa Keselamatan ICT Kementerian.
(49)	JPICT	Jawatankuasa Pemandu ICT Kementerian.
(50)	Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
(51)	Kementerian	Kementerian Sains, Teknologi dan Inovasi (MOSTI).
(52)	Kerajaan	Kerajaan Malaysia yang di wakili oleh Kementerian.
(53)	Kerentanan	Kelemahan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
(54)	Ketua Agensi	Ketua Pengarah dan Ketua Pegawai Eksekutif jabatan-jabatan di bawah Kementerian.
(55)	Koordinator PKP	Pegawai bertanggungjawab menguruskan dan melaksanakan Pelan Kesinambungan Perkhidmatan (PKP) Kementerian.
(56)	Kriptografi	Kaedah untuk menukar data dan maklumat standard kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
(57)	KSU	Ketua Setiausaha Kementerian.
(58)	KU	Ketua Unit.
(59)	LAN	*Local Area Network.* Rangkaian Kawasan Setempat.
(60)	*Lock*	Mengunci komputer.
(61)	Maklumat Terperingkat	Dokumen/Maklumat Rasmi yang dikategorikan sebagai Rahsia Besar, Rahsia, Sulit atau Terhad yang terkandung dalam Arahan Keselamatan.

Bil.	Istilah	Penerangan
(62)	*Malicious Code*	Perkakasan atau perisian yang dimasukkan ke datam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
(63)	*Malware*	Merujuk kepada virus, *worms, trojan horses*, *bots* dan lain-lain kod jahat.
(64)	Media Storan	Semua jenis medium yang berkaitan dengan penyimpanan data dan maklumat seperti telefon bimbit, kad memori, disket, katrij, cakera padat, cakera mudah alih, pita, cakera keras, pemacu pena dan storan awan (*cloud storage*).
(65)	*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.
(66)	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
(67)	Pasukan ERT	*Emergency Response Team.* Pasukan Tindakan Kecemasan.
(68)	Pasukan Komunikasi Krisis	Pasukan yang memastikan ketersediaan keupayaan komunikasi sepanjang berlakunya sesuatu krisis.
(69)	Pasukan Pemulihan Bencana ICT	Pasukan yang terlibat di dalam operasi pemulihan akibat daripada terjadinya sesuatu bencana ICT.
(70)	Pegawai Aset	Pegawai yang dilantik untuk menjaga dan menguruskan aset di Ibu Pejabat Kementerian.
(71)	Pegawai Aset ICT	Pegawai yang dilantik untuk menjaga dan menguruskan aset ICT di Ibu Pejabat Kementerian.
(72)	Pegawai Keselamatan Kementerian	Pegawai yang menjalankan tugas menyedia dan memastikan keselamatan personel dan fizikal di Ibu Pejabat Kementerian.

Bil.	Istilah	Penerangan
(73)	Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
(74)	Pegawai Keselamatan Aras	Pegawai yang dilantik di setiap aras di Kementerian bagi menjamin keselamatan persekitaran tempat kerja.
(75)	Pegawai yang Bertanggungjawab	Pegawai yang diberikan tanggungjawab melaksanakan sesuatu tugas.
(76)	Pelawat	Individu atau kumpulan yang datang berurusan di Kementerian secara rasmi atau tidak rasmi.
(77)	Pemilik Projek	Pihak yang memiliki dan bertanggungjawab kepada projek tersebut.
(78)	Pengguna	Pegawai tetap, pegawai kontrak, pekerja sambilan harian (PSH) dan pelajar latihan industri.
(79)	Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
(80)	Pentadbir Sistem ICT	Pegawai yang diberikan tanggungjawab mengawal selia semua aktiviti sistem di bawah seliaan samada dibangunkan secara *inhouse* atau *outsource* di Kementerian.
(81)	Pentadbir Pusat Data	Pegawai yang mengurus dan mentadbir pengoperasian Pusat Data.
(82)	Pentadbir Rangkaian	Pegawai yang mengurus dan mentadbir sistem rangkaian.
(83)	Pentadbir Teknikal ICT	Pegawai yang mengurus perkakasan dan perisian ICT.
(84)	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.
(85)	Pihak Ketiga	Pihak yang membekalkan atau menerima perkhidmatan Kementerian.

Bil.	Istilah	Penerangan
(86)	PII	*Personal Identifiable Information* - Privasi dan Perlindungan Maklumat Peribadi.
(87)	PKI	*Public-Key Infrastructure.* Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
(88)	PKP	*Business Continuity Planning.* Pelan Kesinambungan Perkhidmatan.
(89)	*Rollback*	Pengunduran. Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
(90)	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
(91)	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
(92)	Ruang siber	Sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengen sistemsistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT.
(93)	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
(94)	*Server*	Pelayan komputer.
(95)	Sokongan Teknikal Kementerian	Khidmat sokongan dan bantuan teknikal ICT di MOSTI.
(96)	*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.
(97)	SUB	Setiausaha Bahagian Kementerian.

Bil.	Istilah	Penerangan
(98)	SUBK(P)	Setiausaha Bahagian Kanan (Pengurusan) Kementerian.
(99)	*Switches*	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.
(100)	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat bermotif personal dan atas sebab tertentu.
(101)	UPS	*Uninterruptible Power Supply.* Peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
(102)	*Video Conference*	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa yang sama ia diterima oleh penghantar.
(103)	*Video Streaming*	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
(104)	Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
(105)	WAN	*Wide Area Network.* Rangkaian yang merangkumi kawasan yang luas.
(106)	Warga Kementerian	Semua kakitangan kerajaan yang berkhidmat di MOSTI samada berjawatan tetap atau kontrak tidak termasuk pelajar praktikal.
(107)	*Wireless* LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
(108)	*Worm*	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

PENGENALAN

TUJUAN

Polisi Keselamatan Siber (PKS), Kementerian Sains, Teknologi dan Inovasi (MOSTI) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga Kementerian, pihak ketiga termasuk pembekal serta pakar runding, dan mana-mana pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian dalam melindungi dan menjamin keselamatan maklumat di persekitaran siber.

LATAR BELAKANG

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

OBJEKTIF

Objektif utama PKS MOSTI ini dibangunkan adalah seperti berikut:

(a) Menerangkan kepada semua pengguna merangkumi warga Kementerian, pihak ketiga termasuk pembekal serta pakar runding, dan mana-mana pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber;

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

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

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

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

SKOP

Polisi ini meliputi semua aset ICT yang digunakan seperti maklumat (contoh: fail, dokumen, data elektronik), perisian (contoh: aplikasi dan pangkalan data) dan fizikal (contoh: Pusat Data, komputer, *server*, peralatan komunikasi dan lain-lain). Dasar ini adalah terpakai kepada semua pengguna di Kementerian termasuk pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, memuat naik, menyedia, berkongsi, menyimpan dan menggunakan aset ICT Kementerian.

PRINSIP

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

(a) **Akses atas dasar perlu mengetahui**

Akses kepada penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan.

(b) **Hak akses minimum**

Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan daripada pegawai yang diberi kuasa adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah, membatalkan atau mencetak sesuatu maklumat.

Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas atau perubahan polisi Kementerian.

(c) **Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT Kementerian.

(d) **Pengasingan**

Tugas mewujud, memadam, menambah, mengubah dan mengesahkan data/maklumat perlu diasingkan. Ini adalah untuk mengelakkan akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi.

(e) **Pengauditan**

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti PC, server, peralatan rangkaian serta keselamatan dan sebagainya hendaklah dipastikan dapat menjana dan menyimpan log untuk tujuan *audit trail*.

(f) **Pematuhan**

PKS MOSTI hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk ketidakpatuhan ke atasnya yang boleh membawa ancaman kepada keselamatan siber.

(g) **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimakan sebarang gangguan atau kerugian perkhidmatan akibat daripada *unavailability* sistem. Pemulihan boleh dilakukan melalui kaedah *redundancy* dan mewujudkan Pelan Kesinambungan Perkhidmatan (PKP), Pelan Teknikal Pemulihan Bencana

(*Disaster Recovery Technical Plan* - DRTP) dan Pelan Pengurusan Pemulihan Bencana (*Disaster Recovery Management Plan* - DRMP).

(h) **Saling Bergantungan**

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

TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS MOSTI, Jawatankuasa Keselamatan ICT (JKICT) Kementerian adalah merupakan struktur tadbir urus yang digunapakai. Keahlian jawatankuasa ini adalah seperti berikut:

(a) Pengerusi : Pegawai Keselamatan ICT (ICTSO) Kementerian

(b) Ahli : Semua Pegawai dan Penolong Pegawai Teknologi Maklumat di Ibu Pejabat Kementerian.

(c) Urus Setia : Seksyen Operasi, Rangkaian dan Keselamatan, Bahagian Pengurusan Teknologi Maklumat MOSTI

(d) Peranan dan tanggungjawab:

i. Merancang, melaksana dan memantau polisi dan dasar keselamatan ICT Kementerian;

ii. Merancang, melaksana dan memantau strategi keselamatan ICT Kementerian;

iii. Merancang, melaksana dan memantau pengurusan keselamatan ICT Kementerian;

iv. Merancang, melaksana dan memantau pelan tindakan keselamatan ICT Kementerian;

v. Menyelaras, melaksana dan memantau dasar, strategi, pelan tindakan dan pengurusan keselamatan ICT;

vi. Mengkaji dan menilai teknologi yang bersesuaian terhadap keperluan keselamatan ICT;

vii. Menjalankan penilaian ke atas tahap keselamatan ICT Kementerian dan mengambil tindakan pengukuhan atau pemulihan;

viii. Mengambil tindakan terhadap sebarang insiden yang dilaporkan;

ix. Mengesyor dan mengambil tindakan yang melibatkan pelanggaran PKS Kementerian; dan/atau

x. Mengesyor dan mengambil tindakan yang melibatkan sebarang insiden keselamatan ICT.

RISIKO

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

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber Kementerian. Penilaian risiko hendaklah dikenalpasti dan dilaksanakan dengan tindakan berikut:

(a) **Kerentanan**

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

(b) **Ancaman**

Kementerian hendaklah mengenalpasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenalpasti.

(c) **Impak**

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

(d) **Tahap Risiko**

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

(e) **Penguraian Risiko**

i. Penguraian risiko hendaklah dikenalpasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos atau faedah.

ii. Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

- Teknologi
  Teknologi hendaklah dikenalpasti untuk mengurangkan risiko. Sebagai contoh, penghadang digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

- Proses
  Perakayasaan proses, Prosedur Operasi Standard (SOP) dan polisi hendaklah dikenalpasti untuk mengurangkan risiko.

- Manusia
  Mengenalpasti sumber manusi berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

(f) **Pengurusan Risiko**

i. Tahap risiko

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

- Mengenalpasti kerentanan;
- Mengenalpasti ancaman;
- Menilai risiko;
- Menentukan penguraian risiko;
- Memantau keberkesanan penguraian risiko; dan
- Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

ii. Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun.

PENYATAAN POLISI

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 siber sentiasa berubah.

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

(a) **Kerahsiaan**

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

(b) **Integriti**

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

(c) **Tidak Boleh Disangkal**

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

(d) **Kesahihan**

Data dan maklumat hendaklah dipastikan kesahihannya.

(e) **Ketersediaan**

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

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

14 bidang keselamatan berikut adalah merupakan prinsip-prinsip yang menjadi asas kepada PKS MOSTI dan perlu dipatuhi iaitu:

BIDANG A.1 : POLISI KESELAMATAN MAKLUMAT

A.1.1 Hala Tuju Pengurusan Untuk Keselamatan Maklumat	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Kementerian dan perundangan yang berkaitan.	
A.1.1.1 Polisi Keselamatan Maklumat	**Peranan**
Ketua Setiausaha (KSU) adalah bertanggungjawab ke atas pelaksanaan arahan dengan dibantu oleh JPICT, JKICT dan CSIRT Kementerian yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Setiausaha Bahagian/Ketua Unit/Pengarah dan ahli-ahli yang dilantik. PKS MOSTI mestilah dibaca, difahami dan dipatuhi oleh semua Warga Kementerian, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian bagi mengelakkan sebarang bentuk ketidakpatuhan ke atasnya yang boleh membawa ancaman kepada keselamatan. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan kepada Warga Kementerian, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian.	JPICT, JKICT, CSIRT, CDO, ICTSO dan SUB/KU/ Pengarah
A.1.1.2 Kajian Semula Polisi Untuk Keselamatan Maklumat	**Peranan**
Polisi ini perlu disemak dan dipinda mengikut keperluan semasa atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan. Berikut ialah prosedur yang berkaitan dengan kajian semula PKS MOSTI: (a) Mengenal pasti dan menentukan perubahan yang diperlukan; (b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan;	JPICT, CDO dan ICTSO

(c)	Memaklumkan pindaan yang telah disahkan oleh JPICT kepada Warga Kementerian, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian; dan	
(d)	Polisi ini hendaklah dikaji semula sekurang-kurangnya setiap lima (5) tahun atau mengikut keperluan semasa bagi memastikan pemakaian dokumen sentiasa relevan.	

BIDANG A.2 : PERANCANGAN BAGI KESELAMATAN ORGANISASI

A.2.1 Pengasingan Tugas	**Peranan**
Objektif: Menerangkan tentang pengasingan tugas, peranan dan tanggungjawab individu yang terlibat.	
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; (c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan (d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	SUB BPTM
A.2.2 Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS MOSTI.	

A.2.2.1 Peranan dan Tanggungjawab Keselamatan Maklumat	Peranan
(a) Ketua Setiausaha (KSU) Peranan dan tanggungjawab adalah seperti yang berikut:. i. Memastikan penguatkuasaan pelaksanaan PKS MOSTI; ii. Memastikan Warga Kementerian, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian membaca, memahami dan mematuhi peruntukan-peruntukan di bawah polisi ini; iii. Memastikan semua keperluan Kementerian seperti sumber kewangan dan personel adalah mencukupi; iv. Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan; dan v. Melantik CDO dan ICTSO.	KSU
(b) Ketua Pegawai Digital (CDO) Peranan dan tanggungjawab adalah seperti yang berikut: i. Meneraju penggunaan data, analitis dan teknologi berfokuskan organisasi dalam bidang teknologi digital, insfrstruktur data dan tadbir urus data; ii. Mentransformasi perkhidmatan digital (produk dan perkhidmatan) sebagai *innovator strategist* dan *data-driven strategist* berfokuskan perkhidmatan Kerajaan dan pengguna terutamanya yang melibatkan analitik data, literasi digital dan platform perkhidmatan kendiri atau layan diri; iii. Mentransformasi pengalaman pelanggan sebagai inovator pemacu data (*data-driven innovator*) berfokuskan *Whole-of-Government* terutamanya melibatkan perkongsian data, data terbuka, teknologi baharu, teknologi pintar dan perkhidmatan digital antara agensi/bahagian di bawah kawal selia;	SUBK(P)

iv. Menilai, menyelaras, memperaku keperluan perkhidmatan digital, rekabentuk perkhidmatan teknikal dan peruntukan pembangunan serta mengurus agensi sebagai pelaksana inisiatif dan projek pendigitalan; v. Meneraju perubahan melalui penjajaran Pelan Strategik Pendigitalan (PSP) Kementerian/Negeri/Agensi dengan: ● Memastikan PSP Kementerian selari dengan PSP Sektor Awam dan Pengurusan Risiko serta Pelan Pengurusan Perubahan; dan ● Memantapkan struktur tadbir urus pendigitalan agensi dan menyelaras penggunaan dasar, garis panduan dan amalan terbaik global.	
(c) Pegawai Keselamatan ICT (ICTSO) Peranan dan tanggungjawab ICTSO adalah seperti yang berikut: i. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS MOSTI; ii. Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling, garis panduan dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; iii. Menyedia dan menyebarkan program kesedaran yang sesuai mengenai ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; iv. Melaporkan insiden keselamatan siber mengikut keutamaan: ● Keutamaan 1: Melaporkan insiden keselamatan siber kepada CDO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP). Pengurusan dan pengendalian insiden dilaksana tertakluk kepada PKP dan Agensi Keselamatan Siber	SUB BPTM

Negara (NACSA) di bawah Majlis Keselamatan Negara (MKN); ● Keutamaan 2: Melaporkan insiden keselamatan siber kepada CSIRT Kementerian dan seterusnya memaklumkan kepada CDO serta NACSA. Pengurusan dan pengendalian insiden dilaksanakan secara kendiri. v. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; vi. Melaksanakan pematuhan polisi oleh Warga Kementerian, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian; vii. Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; dan viii. Menyedia dan merangka latihan dan program kesedaran keselamatan siber.	
(d) Pengurus ICT Peranan dan tanggungjawab Pengurus ICT ialah melaksanakan keperluan Polisi ini dalam operasi semasa seperti yang berikut: i. Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; ii. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa; iii. Menetukan tahap keutamaan insiden; iv. Melaporkan insiden kepada CSIRT; dan	SUB BPTM

v. Menetapkan dan mengambil langkah-langkah pemulihan awal.	
(e) Pentadbir Sistem ICT Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti yang berikut: i. Mengambil tindakan yang bersesuaian apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; ii. Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam polisi ini; iii. Memantau aktiviti capaian sistem aplikasi; iv. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; v. Menganalisis dan menyimpan rekod jejak audit; vi. Menyediakan laporan mengenai aktiviti capaian secara berkala; dan vii. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel di dalam keadaan yang baik.	Pentadbir Sistem ICT
(f) Jawatankuasa Pemandu ICT (JPICT) Kementerian Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil 3 Tahun 2015. JPICT adalah jawatankuasa yang bertanggungjawab dalam hala tuju atau dasar keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam Kementerian. Bidang kuasa: i. Memperaku/meluluskan dokumen PKS Kementerian;	JPICT

ii. Memperaku garis panduan, prosedur dan tatacara berkaitan ICT yang mematuhi keperluan PKS Kementerian; iii. Memperaku teknologi yang bersesuaian dilaksanakan di Kementerian; iv. Memastikan PKS Kementerian adalah selari dengan dasar-dasar ICT yang sedang berkuat kuasa; dan v. Menerima laporan keselamatan ICT daripada JKICT Kementerian bagi memastikan keselamatan ICT adalah selamat dan terjamin.	
(g) Jawatankuasa Keselamatan ICT (JKICT) Kementerian Peranan dan tanggungjawab JKICT Kementerian adalah seperti berikut: i. Merancang, melaksana dan memantau polisi dan dasar keselamatan ICT Kementerian; ii. Merancang, melaksana dan memantau strategi keselamatan ICT Kementerian; iii. Merancang, melaksana dan memantau pengurusan keselamatan ICT Kementerian; iv. Merancang, melaksana dan memantau pelan tindakan keselamatan ICT Kementerian; v. Menyelaras, melaksana dan memantau dasar, strategi, pelan tindakan dan pengurusan keselamatan ICT; vi. Mengkaji dan menilai teknologi yang bersesuaian terhadap keperluan keselamatan ICT; vii. Menjalankan penilaian ke atas tahap keselamatan ICT Kementerian dan mengambil tindakan pengukuhan atau pemulihan; viii. Mengambil tindakan terhadap sebarang insiden yang dilaporkan;	JKICT

ix. Mengesyor dan mengambil tindakan yang melibatkan pelanggaran PKS Kementerian; dan x. Mengesyor dan mengambil tindakan yang melibatkan sebarang insiden keselamatan siber.	
(h) Pengguna Peranan dan tanggungjawab pengguna adalah seperti yang berikut: i. Membaca, memahami dan mematuhi polisi ini; ii. Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya; iii. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; iv. Melaksanakan prinsip-prinsip keselamatan polisi ini dan menjaga kerahsiaan maklumat Kerajaan; v. Melaksanakan langkah-langkah perlindungan seperti yang berikut: ● Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ● Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; ● Menentukan maklumat sedia untuk digunakan; ● Menjaga kerahsiaan maklumat; ● Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan; ● Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan	Pengguna

● Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum. vi. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT Kementerian dengan segera; vii. Menghadiri program-program kesedaran mengenai keselamatan siber; dan viii. Bersetuju dengan terma dan syarat yang terkandung di dalam polisi ini.	
A.2.3 Organisasi Luaran	
Objektif: Memastikan hubungan yang baik dengan pihak berkuasa berkaitan bagi melancarkan proses komunikasi.	
A.2.3.1 Hubungan Dengan Pihak Berkuasa	**Peranan**
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab Kementerian; (b) Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Di-Raja Malaysia (PDRM) dan Suruhanjaya Komunikasi Multimedia Malaysia (SKMM). Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, penyedia perkhidmatan kecemasan, elektrik, keselamatan dan kesihatan serta pihak bomba; dan (c) Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	SUB, Pemilik Projek dan Pihak Ketiga

A.2.3.2 Hubungan Dengan Kumpulan Berkepentingan Khusus/Istimewa	**Peranan**
Hubungan baik dengan kumpulan berkepentingan yang khusus/ istimewa atau forum bersama pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau 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.	Warga Kementerian
A.2.3.3 Keselamatan Maklumat Dalam Pengurusan Projek	**Peranan**
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek Kementerian; (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;	Warga Kementerian

(d) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung di dalam polisi Kementerian; dan (e) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.	
A.2.4 Komunikasi Lain	
A.2.4.1 Peranti Mudah Alih dan Telekerja	
Objektif: Memastikan keselamatan telekerja dan penggunaan peralatan mudah alih.	
A.2.4.1.1 Polisi Peranti Mudah Alih (*Mobile Device Policy*)	**Peranan**
(a) Membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih.	Sokongan Teknikal Kementerian
(b) Meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih.	JPICT
(c) Perkara-perkara yang perlu dipatuhi: i. Pendaftaran ke atas peralatan mudah alih; ii. Keperluan ke atas perlindungan secara fizikal; iii. Kawalan ke atas pemasangan perisian peralatan; iv. Kawalan ke atas versi dan *patches* perisian; v. Sekatan ke atas akses perkhidmatan maklumat secara dalam talian; vi. Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan vii. Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.	Warga Kementerian

A.2.4.1.2 Telekerja (*Teleworking*)	**Peranan**
Prosedur atau tatacara keselamatan sokongan hendaklah dilaksana dan dipatuhi bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja. Pelaksanaannya hendaklah mematuhi Dasar Bekerja Dari Rumah (rujuk garis panduan dan pekeliling Jabatan Perkhidmatan Awam).	Warga Kementerian

BIDANG A.3: KESELAMATAN SUMBER MANUSIA

A.3.1 Sebelum Perkhidmatan	
Objektif: Memastikan semua pengguna dan pihak ketiga yang mempunyai urusan dengan perkhidmatan Kementerian memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset.	
A.3.1.1 Tapisan Keselamatan	**Peranan**
Tapisan keselamatan hendaklah dijalankan terhadap semua pengguna dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT Kementerian yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pengguna serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan (b) Menjalankan tapisan keselamatan untuk pegawai dan pengguna berasaskan keperluan perundangan, peraturan dan etika terpakai selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Pengguna dan Pihak Ketiga
A.3.1.2 Terma dan Syarat Perkhidmatan	**Peranan**
Persetujuan berkontrak dengan warga Kementerian, pengguna dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT Kementerian hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pengguna serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;	ICTSO, Pengguna dan Pihak Ketiga

(b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani; dan (c) Menyediakan dokumen keselamatan yang berkaitan seperti Borang Pematuhan *Non Disclosure Agreement* (NDA) untuk ditandatangani oleh pengguna dan pihak ketiga.	
A.3.2 Dalam Tempoh Perkhidmatan	
Objektif: Memastikan warga Kementerian, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.	
A.3.2.1 Tanggungjawab Pengurusan	**Peranan**
Pengurusan hendaklah memastikan warga Kementerian, pengguna dan pihak ketiga supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	ICTSO, Pengguna dan Pihak Ketiga
A.3.2.2 Program Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat	**Peranan**
Warga Kementerian, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber Kementerian, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/	ICTSO, Pengguna dan Pihak Ketiga

sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; (b) Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber Kementerian 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.	
A.3.2.3 Proses Tatatertib	**Peranan**
Proses tatatertib yang formal dan disampaikan kepada warga Kementerian hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga Kementerian yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga Kementerian sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh Kementerian; dan (b) Warga Kementerian yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT Kementerian.	Unit Integriti
A.3.3 Penamatan dan Pertukaran Perkhidmatan	
Objektif: Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas warga Kementerian diurus dengan teratur.	
A.3.3.1 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan	**Peranan**
Tindakan yang perlu diambil setelah menerima notifikasi pegawai yang bertukar keluar atau menamatkan perkhidmatan adalah seperti berikut:	Pentadbir Sistem ICT, Pengguna

(a)	Memastikan semua aset ICT dikembalikan kepada Kementerian 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 Kementerian dan/atau terma perkhidmatan yang ditetapkan; dan	
(c)	Maklumat rahsia rasmi Kementerian dalam peranti tidak dibenarkan dibawa keluar dari Kementerian.	

BIDANG A.4 : PENGURUSAN ASET

A.4.1 Tanggungjawab Terhadap Aset	
Objektif: Untuk mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Kementerian.	
A.4.1.1 Inventori Aset	Peranan
Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT Kementerian. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal, sistem pengurusan aset Kementerian; (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; (d) Pegawai Aset hendaklah mengesahkan penempatan aset ICT; (e) Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala . berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; (f) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan (g) Memastikan semua aset ICT sentiasa dikemas kini di dalam Sistem Pengurusan Aset.	Pegawai Aset ICT dan Pegawai yang Bertanggungjawab

A.4.1.2 Pemilikan Aset	**Peranan**
Aset ICT adalah hak milik Kementerian. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut: (a) Memastikan penerimaan set dan senarai aset di bawah tanggungjawabnya dikemaskini; (b) Memastikan aset telah dikelaskan dan dilindungi; (c) Memastikan pemilik aset mematuhi polisi kawalan capaian yang telah ditetapkan; dan (d) Memastikan semua jenis aset dipelihara dengan baik.	Pegawai Aset ICT dan Warga Kementerian
A.4.1.3 Penggunaan Aset yang Dibenarkan	**Peranan**
Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	Warga Kementerian
A.4.1.4 Pemulangan Aset	**Peranan**
Warga Kementerian hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	Warga Kementerian
A.4.2 Pelaksanaan Pengelasan Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
A.4.2.1 Pengelasan Maklumat	**Peranan**
Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.	Pegawai Pengelasan
A.4.2.2 Pelabelan Maklumat	**Peranan**
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.	Warga Kementerian

A.4.2.3 Pengendalian Aset	**Peranan**
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah bagi **kategori fizikal** 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) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (e) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; (f) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum; (g) Maklumat terperingkat Kementerian yang disimpan secara fizikal tidak boleh disimpan melebihi tempoh yang ditetapkan; (h) Maklumat terperingkat Kementerian hendaklah dilupuskan dengan kaedah yang selamat apabila tidak lagi diperlukan. Ini adalah untuk mengelakkan daripada pendedahan maklumat rasmi Kerajaan dan maklumat sensitif seperti *Personal Identifiable Information (*PII*)* kepada pihak yang tidak dibenarkan; dan (i) Kementerian hendaklah memastikan rekod pelupusan disimpan sebagai bukti.	Warga Kementerian

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah bagi **kategori digital** hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Aset perlu mempunyai kata laluan; (b) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (c) Memberikan perhatian kepada maklumat terperingkat terutamanya semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, pnghantaran, penyampaian, pertukaran dan pemusnahan; (d) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum; (e) Menggunakan medium rasmi yang dibenarkan; (f) Maklumat terperingkat Kementerian yang disimpan secara elektronik tidak boleh disimpan melebihi tempoh yang ditetapkan; (g) Maklumat terperingkat Kementerian yang disimpan secara elektronik hendaklah dihapuskan dengan kaedah yang selamat apabila tidak lagi diperlukan. Ini adalah untuk mengelakkan daripada pendedahan maklumat rasmi Kerajaan dan maklumat sensitif seperti PII kepada pihak yang tidak dibenarkan; dan (h) Kementerian hendaklah memastikan rekod pelupusan disimpan sebagai bukti.	

A.4.2.4 Pemadaman Maklumat	Peranan
Maklumat yang disimpan di dalam sistem aplikasi, peralatan atau apa-apa media simpanan hendaklah dipadamkan apabila ia tidak lagi diperlukan. Ini adalah bagi mengelakkan maklumat sensitif terdedah dengan mudah dan untuk memastikan pemadaman maklumat adalah mematuhi undang-undang, garis panduan atau apa-apa keperluan kontrak.	Pengguna, Pentadbir Sistem ICT dan ICTSO
A.4.3 Pengendalian Media	
Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
A.4.3.1 Pengurusan Media Boleh Alih	**Peranan**
Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh Kementerian. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (e) Menyimpan semua jenis media di tempat yang selamat.	Pentadbir Sistem ICT dan Pengguna

A.4.3.2 Pelupusan Media	Peranan
(a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan. (b) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset
A.4.3.3 Pemindahan Media Fizikal	**Peranan**
(a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan. (b) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset
A.4.4 Kebocoran Data	
Objektif: Mengenalpasti dan mencegah pendedahan dan pengekstrakan maklumat yang tidak dibenarkan samada oleh individu atau melalui sistem.	
A.4.4.1 Pencegahan Kebocoran Data	**Peranan**
Kementerian hendaklah mempertimbangkan perkara berikut bagi mengurangkan risiko kebocoran data (contoh maklumat peribadi): (a) Mengenal pasti dan mengelaskan maklumat sensitif untuk melindunginya daripada kebocoran data pada sistem, rangkaian dan *end-point devices*; (b) Memantau saluran-saluran kebocoran data Kementerian seperti pemindahan fail, peranti mudah alih dan peranti storan mudah alih; (c) Pemantauan dan mengehadkan kebolehan pengguna daripada menyalin, menampal dan memuat naik maklumat sensitif keatas perkhidmatan, peralatan atau storan di luar Kementerian boleh dilakukan dengan menggunakan	Pegawai Teknikal ICT Pentadbir Rangkaian Pentadbir Pusat Data Pentadbir Sistem

	perisian khusus yang sesuai; dan	
(d)	Melaksanakan program kesedaran kepada warga Kementerian sebagai langkah pencegahan bagi kebocoran data.	

BIDANG A.5 : KAWALAN AKSES

A.5.1 Keperluan Kawalan Akses	
Objektif: Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.	
A.5.1.1 Polisi Kawalan Akses	**Peranan**
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. la perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Keperluan keselamatan aplikasi; (b) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; (c) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; (d) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (e) Pengasingan peranan kawalan capaian; (f) Kebenaran rasmi permintaan akses; (g) Keperluan semakan hak akses berkala; (h) Pembatalan hak akses; (i) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan	ICTSO dan Pentadbir Sistem ICT

(j) Capaian *privilege*.	
A.5.1.2 Capaian Kepada Rangkaian dan Perkhidmatan Rangkaian	**Peranan**
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari Kementerian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian Kementerian, 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.	Pengguna dan Pentadbir Rangkaian
A.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 dasar kawalan capaian pengguna sedia ada.	
A.5.2.1 Pendaftaran dan Pembatalan Pengguna	**Peranan**
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh Kementerian sahaja boleh digunakan; (b) Akaun pengguna mestilah unik; (c) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada Kementerian terlebih dahulu;	Pengguna dan Warga Kementerian

(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 Kementerian.	
A.5.2.2 Peruntukan Akses Pengguna	**Peranan**
Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.	Pentadbir Sistem ICT dan SUB/KU/Pengarah
A.5.2.3 Pengurusan Hak Akses Istimewa	**Peranan**
Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan Skop tugas merujuk kepada Prosedur Pendaftaran dan Penamatan Pengguna.	Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Rangkaian dan ICTSO
A.5.2.4 Pengurusan Maklumat Pengesahan Rahsia Pengguna	**Peranan**
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	ICTSO dan Pentadbir Sistem ICT
A.5.2.5 Kajian Semula / Semakan Hak Akses Pengguna	**Peranan**
Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan. 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.	ICTSO dan Pentadbir Sistem ICT

A.5.2.6 Pembatalan atau Pelarasan Hak Akses	**Peranan**
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 Kementerian.	Pentadbir Sistem ICT dan SUB/KU/Pengarah
A.5.2.7 Menyembunyikan Data (*Data Masking*)	**Peranan**
Maklumat pengesahan rahsia pengguna hendaklah disembunyikan atau dibuat penyulitan bagi mengelakkan pendedahan maklumat kepada pihak yang tidak dibenarkan. Sistem aplikasi yang mewujudkan, memproses, menyimpan, menghantar dan meluluskan maklumat sensitif (contohnya nombor kad pengenalan, PII) hendaklah diberikan penyulitan atau kaedah menyembunyikan data bagi mengehadkan pendedahan data sensitif termasuk maklumat yang boleh dikenalpasti secara peribadi dan untuk mematuhi keperluan undang-undang, berkanun, peraturan dan kontrak.	Pentadbir Sistem ICT dan Pemilik Projek
A.5.3 Tanggungjawab Pengguna	
Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.	
A.5.3.1 Penggunaan Maklumat Pengesahan Rahsia	**Peranan**
Peranan dan tanggungjawab pengguna adalah seperti yang berikut: (a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber Kementerian; (b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; (c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat Kementerian;	Pengguna, Pentadbir Sistem ICT dan SUB/KU/Pengarah

(d) Melaksanakan langkah-langkah perlindungan seperti yang berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum. (e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan siber; dan (g) Membuat permohonan baharu atau permohonan pengaktifan semula akaun selepas akaun digantung atau dibatalkan.	
A.5.3.2 Amalan Penggunaan Maklumat Pengesahan Rahsia	**Peranan**
Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.	Pengguna, Pentadbir Sistem, ICTSO dan SUB/KU/Pengarah

A.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.	
A.5.4.1 Sekatan Akses Maklumat	**Peranan**
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut polisi kawalan akses.	Pengguna, Pentadbir Sistem, ICTSO dan SUB/KU/Pengarah
A.5.4.2 Prosedur Log Masuk yang Selamat	**Peranan**
Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Kementerian; (b) Menjana amaran *(alert)* sekiranya berlaku perlanggaran semasa proses log maşuk terhadap aplikasi sistem; (c) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; (d) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; (e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; (f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem; (g) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;	Pentadbir Sistem, ICTSO dan SUB/KU/Pengarah

(h) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (i) Menghadkan masa tidak aktif semasa di dalam sesi sistem selama lima (5) minit; dan (j) Memastikan kawalan keselamatan sistem rangkaian, aplikasi dan pangkalan data adalah kukuh dan menyeluruh bagi mengelakkan aktiviti atau capaian yang tidak sah.	
A.5.4.3 Sistem Pengurusan Kata Laluan	**Peranan**
Sistem pengurusan kata laluan hendaklah interaktif dan mengambilkira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Kementerian seperti yang 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; (c) Panjang kata laluan mestilah sekurang-kurangnya 12 aksara dengan gabungan 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;	Pentadbir Sistem, ICTSO dan SUB/KU/Pengarah

(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 akaun capaian diaktifkan semula; (j) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna; dan (k) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian.	
A.5.4.4 Penggunaan Program Utiliti yang Mempunyai Hak Istimewa	**Peranan**
Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding System*.	Pentadbir Sistem ICT dan SUB/KU/Pengarah
A.5.4.5 Kawalan Akses Kepada Kod Sumber Program	**Peranan**
Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; (b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan (c) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik Kementerian.	Pemilik Projek, Pihak Ketiga dan Pentadbir Sistem ICT

BIDANG A.6 : KRIPTOGRAFI

A.6.1 Kawalan Kriptografi	
Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan, dan/atau keutuhan maklumat.	
A.6.1.1 Polisi Penggunaan Kawalan Kriptografi	**Peranan**
Kriptografi merangkumi kaedah-kaedah seperti yang berikut: (a) Pengguna hendaklah membuat *encryption* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa; dan (b) Penggunaan tandatangan digital adalah diperlukan sekiranya pengguna menguruskan transaksi maklumat terperingkat secara elektronik.	Pemilik Projek
A.6.1.2 Pengurusan Kunci Awam (*Public Key*)	**Peranan**
Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam atau *Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	ICTSO dan Warga Kementerian

BIDANG A.7 : KESELAMATAN FIZIKAL DAN PERSEKITARAN

A.7.1 Kawasan Selamat	
Objektif: Menghalang akses fizikal yang tidak dibenarkan untuk mengelakkan kecurian, kerosakan atau gangguan kepada maklumat serta gangguan kepada kemudahan pemprosesan maklumat Kementerian.	
A.7.1.1 Perimeter Keselamatan Fizikal	**Peranan**
Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT Kementerian. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (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 Iain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan (g) Memasang alat penggera atau kamera keselamatan.	BT

A.7.1.2 Kawalan Kemasukan Fizikal	**Peranan**
Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis Kementerian. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Setiap pegawai dan kakitangan Kementerian hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada Kementerian apabila bertukar, tamat perkhidmatan atau bersara; (b) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan di kaunter dan mengembalikan semula selepas selesai urusan; (c) Hanya pengguna yang diberikan kebenaran sahaja boleh menggunakan aset ICT Kementerian; dan (d) Kehilangan pas hendaklah dilaporkan segera kepada Pihak Berkuasa.	Warga Kementerian, Pihak Ketiga, Perunding dan Pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian
A.7.1.3 Pemantauan Keselamatan Fizikal	**Peranan**
Akses fizikal ke premis hendaklah dikawal dan dipantau setiap masa daripada pihak yang tidak dikenali atau sebarang aktiviti yang mencurigakan. Langkah-langkah berikut boleh dipertimbangkan bagi pemantauan keselamatan fizikal: (a) Memastikan premis disediakan dengan pemantauan komprehensif seperti Pengawal Keselamatan, alat penggera pencerobohan, *Closed-Circuit Television* (CCTV) dan Sistem Pengurusan Maklumat Keselamatan Fizikal; (b) Sistem pemantauan fizikal hendaklah dilindungi daripada sebarang ancaman yang boleh menjejaskan fungsi atau keselamatan maklumat Kementerian;	Pegawai Keselamatan Kementerian; Pegawai Keselamatan Aras

(c) Pemantauan fizikal hendaklah diuji atau diselenggara secara berkala bagi memastikan ketersediaan fungsinya semasa kecemasan; dan (d) Tempoh pengekalan rekod pemantauan fizikal bagi CCTV dan Sistem Pengurusan Maklumat Keselamatan Fizikal seperti yang telah ditetapkan di dalam prosedur semasa.	
A.7.1.4 Keselamatan Pejabat, Bilik dan Kemudahan	**Peranan**
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data perlu dikawal daripada diakses tanpa kebenaran; (b) Pelan lantai tempat larangan seperti di para (a) haruslah mematuhi arahan keselamatan; dan (c) Petunjuk lokasi bilik operasi dan tempat larangan hendaklah mematuhi Arahan Keselamatan.	Warga Kementerian, Pihak Ketiga, Perunding dan Pihak yang mempunyai urusan dengan perkhidmatan Kementerian
A.7.1.5 Perlindungan Daripada Ancaman Luar dan Persekitaran	**Peranan**
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dikaji, dirangka dan dilaksanakan. Kementerian perlu merancang dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	Pentadbir Pusat Data dan BT
A.7.1.6 Bekerja di Kawasan Selamat	**Peranan**
Prosedur bekerja di kawasan selamat hendaklah dilaksanakan dan dipatuhi. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi Warga Kementerian yang	Pentadbir Pusat Data dan BT

tertentu sahaja bagi melindungi aset ICT yang terdapat dalam premis Kementerian. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Perkara-perkara yang perlu dilindungi adalah seperti berikut: (a) Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; (b) Akses adalah terhad kepada Warga Kementerian yang telah diberi kuasa sahaja dan dipantau pada setiap masa; (c) Pemantauan dibuat menggunakan CCTV atau lain-lain peralatan yang sesuai; (d) Peralatan dan perisian keselamatan (CCTV / log akses) perlu diperiksa secara berjadual; (e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; (f) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; (g) Memperkukuh tingkap dan pintu serta dipastikan ia dikunci untuk mengawal kemasukan; (h) Memperkukuh dinding dan siling; dan (i) Menghadkan jalan keluar masuk.	
A.7.1.7 Kawasan Penyerahan dan Pemunggahan	**Peranan**
Kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada	BT, Warga Kementerian, Pihak Ketiga dan Pihak yang

kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan.	mempunyai urusan dengan perkhidmatan Kementerian
A.7.2 Peralatan ICT	
Objektif: Melindungi peralatan ICT Kementerian daripada kehilangan, kerosakan, kecurian dan disalahgunakan.	
A.7.2.1 Penempatan dan Perlindungan Peralatan ICT	**Peranan**
Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut: (a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (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;	Warga Kementerian, Pihak Ketiga dan Pihak yang mempunyai urusan dengan perkhidmatan Kementerian

(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* (GenSet);	
(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 Kementerian, 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 (t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan Kementerian sahaja.	
A.7.2.2 Utiliti Sokongan	**Peranan**
Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan Iain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).	Warga Kementerian, Pihak Ketiga dan Pihak yang mempunyai urusan dengan perkhidmatan Kementerian
A.7.2.3 Keselamatan Kabel	**Peranan**
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;	BPTM dan BT

(c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	
A.7.2.4 Penyelenggaraan Peralatan	**Peranan**
Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; (c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan (e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pegawai Aset dan BPTM
A.7.2.5 Pengalihan Aset	**Peranan**
Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:	Pengguna dan Pegawai Aset

(a) Peralatan ICT yang hendak dibawa keluar dari premis Kementerian untuk tujuan rasmi, pertulah mendapat kelulusan ICTSO Kementerian atau pegawai yang diperturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan (b) Aktiviti peminjaman dan pemulangan aset ICT mestilah direkodkan oleh pegawai yang berkenaan.	
A.7.2.6 Keselamatan Peralatan dan Aset di Luar Premis	**Peranan**
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira . pelbagai risiko bekerja di luar premis Kementerian. Peralatan yang dibawa keluar dari premis Kementerian adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Warga Kementerian, Pihak Ketiga dan Pihak yang mempunyai urusan dengan perkhidmatan Kementerian
A.7.2.7 Pelupusan yang Selamat atau Penggunaan Semula Peralatan	**Peranan**
Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (*overwrite*) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Kementerian dan ditempatkan di Kementerian. Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan	Pegawai Aset dan Warga Kementerian

secara terkawal dan lengkap supaya maktumat tidak terlepas daripada kawalan Kementerian. Langkah-langkah seperti yang berikut hendaklah diambil: (a) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat; (b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (d) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; (e) Pengguna ICT adalah dilarang daripada melakukan perkara-perkara berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM, hardisk, motherboard* dan sebagainya; iii. Menyimpan dan memindahkan perkakasan luaran komputer seperti *Automatic Voltage Regulator* (AVR), *speaker* dan mana-mana peralatan ICT yang berkaitan ke mana-mana bahagian di Kementerian; iv. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan	

v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggungjawab Kementerian. (f) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti Pemacu Kilat USB (*ThumbDrive, PenDrive*) sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; (g) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. (h) Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan; (i) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan yang berkuat kuasa; (j) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan (k) Pegawai aset bertanggungjawab hendaklah merekod maklumat pelupusan dan mengemas kini rekod pelupusan di dalam sistem.	
A.7.2.8 Peralatan Pengguna Tanpa Kawalan	**Peranan**
Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: (a) Tamatkan sesi aktif apabila selesai tugas;	Warga Kementerian, Pihak Ketiga dan Pihak yang mempunyai urusan dengan perkhidmatan Kementerian

(b) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan (c) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	
A.7.2.9 Polisi Meja Kosong dan Skrin Kosong	**Peranan**
Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Pelaksanaan polisi ini bermaksud pengguna tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada di atas meja atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuklah seperti yang berikut: (a) Menggunakan kemudahan *password screensaver* atau *logout* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat. (d) E-mel masuk dan keluar hendaklah dikawal; dan (e) Mengawal penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	Warga Kementerian
A.7.2.10 *Bring Your Own Device* (BYOD)	**Peranan**
BYOD merupakan peralatan mudah alih persendirian seperti telefon pintar, *tablet* atau komputer riba yang digunakan untuk melaksanakan tugasan rasmi Kerajaan.	Pengguna dan Pentadbir Rangkaian

Kawalan adalah merangkumi pengguna yang menggunakan kemudahan sistem rangkaian internet Kerajaan atau persendirian. Setiap pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD iaitu: (a) Mengelakkan risiko kebocoran maklumat rahsia rasmi; (b) Mengelakkan ancaman risiko keselamatan siber; (c) Memastikan produktiviti tidak terjejas dalam menjalankan urusan rasmi jabatan; dan (d) Meningkatkan integriti data. Bagi mengawal dan memantau pelaksanaan BYOD, mekanisme kawalan diwujudkan seperti berikut: (a) Mendaftarkan penggunaan peralatan mudah alih yang digunakan; (b) Mengaktifkan fungsi keselamatan kata laluan bagi mengelakkan akses yang tidak dibenarkan; dan (c) Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan. Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.	

BIDANG A.8 : KESELAMATAN OPERASI

A.8.1 Prosedur dan Tanggungjawab Operasi	
Objektif: Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat.	
A.8.1.1 Prosedur Operasi yang Didokumenkan	**Peranan**
Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut: (a) Semua prosedur keselamatan siber yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pentadbir Sistem ICT
A.8.1.2 Pengurusan Perubahan	**Peranan**
Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen	Pentabir Sistem ICT

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.	
A.8.1.3 Pengurusan Kapasiti	**Peranan**
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah 5mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan (b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pemilik Projek dan Pentadbir Sistem ICT
A.8.1.4 Pengurusan Konfigurasi	**Peranan**
Konfigurasi perkakasan, perisian, perkhidmatan (contoh pengkomputeran awan) dan rangkaian perlu diwujudkan, didokumenkan, dilaksanakan, dipantau dan disemak. Ini bagi memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi seperti mana yang ditetapkan dan konfigurasinya	Pentadbir Rangkaian Pentadbir Pusat Data Pentadbir Aplikasi

adalah tepat dan tidak berubah tanpa kebenaran.	Pentadbir Teknikal ICT
A.8.1.5 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi	**Peranan**
Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*); dan (b) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.	Pentadbir Sistem ICT
A.8.2 Perlindungan Daripada Perisian Hasad (*Malware*)	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada perisian hasad.	
A.8.2.1 Kawalan Daripada Perisian Hasad	**Peranan**
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan perisian hasad 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 perisian hasad seperti antivirus, *Web Application Firewall* (WAF), *Intrusion Detection System*	Pengguna dan Pentadbir Sistem ICT

(IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; (d) Mengemas kini antivirus dengan paten antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala atau mengikut keperluan bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Melibatkan diri dalam 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.	
A.8.2.2 Saringan Web	**Peranan**
Akses kepada laman web luaran yang ditegah oleh Kementerian hendaklah disekat/disaring bagi mengurangkan keterdedahan kepada sebarang bentuk ancaman daripada perisian jahat (*malicious content*) serta sumber laman web yang tidak dibenarkan.	JDN Pentadbir Rangkaian
A.8.3 Sandaran (*Backup*)	
Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.	

A.8.3.1 Sandaran Maklumat	Peranan
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dipulihkan setelah berlakunya bencana, sandaran hendaklah direkodkan dan disimpan di *off-site*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Membuat sandaran keselamatan ke atas semua data. Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan atau bulanan. Kekerapan sandaran bergantung kepada tahap kritikal maklumat; dan (b) Pengujian terhadap sistem sandaran sedia ada hendaklah dilaksanakan bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana.	Pentadbir Sistem ICT
A.8.4 Pengelogan (*Logging*) dan Pemantauan	
Objektif: Merekodkan peristiwa dan menghasilkan bukti	
A.8.4.1 Pengelogan Kejadian (*Event Logging*)	**Peranan**
Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log	Pentadbir Sistem ICT

bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: (a) Fail log sistem pengoperasian; (b) Fail log servis; (c) Fail log aplikasi (*audit trail*); dan (d) Fail log rangkaian. Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada pasukan CSIRT Kementerian.	
A.8.4.2 Perlindungan Maklumat Log	**Peranan**
Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.	Pentadbir Sistem ICT
A.8.4.3 Log Pentadbir dan Pengendali	**Peranan**
Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula 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	Pentadbir Sistem ICT

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 pasukan CSIRT Kementerian.	
A.8.4.4 Penyeragaman Waktu	**Peranan**
Waktu (jam dan minit) bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah . domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Kementerian atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM).	Pentadbir Pusat Data
A.8.4.5 Aktiviti Pemantauan	**Peranan**
Aktiviti rangkaian, sistem dan aplikasi hendaklah dipantau untuk mengenalpasti tindakan anomali yang berlaku. Ia adalah bagi membolehkan tindakan sewajarnya dapat diambil untuk menilai potensi insiden keselamatan maklumat. Skop dan tahap pemantauan ditentukan mengikut keperluan organisasi dan undang-undang serta peraturan yang berkaitan. Rekod dan maklumat pemantauan hendaklah disimpan dalam tempoh masa yang sesuai. Rekod dan maklumat pemantauan adalah seperti:	Pentadbir Sistem ICT dan Pihak Ketiga

(a) Trafik keluar masuk maklumat rangkaian, sistem dan aplikasi; (b) Akses kepada sistem, server, peralatan rangkaian, sistem pemantauan, sistem-sistem kritikal dan lain-lain; (c) Fail konfigurasi sistem dan rangkaian pelbagai peringkat; (d) Log peralatan rangkaian; (e) Log kejadian (*events log*) berkaitan aktiviti sistem dan rangkaian; (f) Semakan kod yang sedang digunakan hendaklah kod yang dibenarkan ke atas sistem dan tidak mengganggu operasi sistem; dan (g) Penggunaan sumber dan prestasinya.	
A.8.5 Kawalan Perisian yang Beroperasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
A.8.5.1 Pemasangan / Naik Taraf Perisian Pada Sistem yang Sedang Beroperasi	**Peranan**
Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem yang sedang beroperasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut: (a) Merancang keperluan *rollback* yang 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.	Pentadbir Sistem ICT

A.8.6 Pengurusan Kerentanan (*Vulnerability*) Teknikal	
Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
A.8.6.1 Pengurusan Kerentanan Teknikal	**Peranan**
Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah dinilai dan langkah-langkah yang sesuai perlu 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: (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.	Pentadbir Sistem ICT
A.8.6.2 Sekatan Ke Atas Pemasangan Perisian	**Peranan**
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 Kementerian, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; dan (d) Pengguna hendaklah mendapat kebenaran daripada Pengurus ICT untuk membuat instalasi perisian tambahan.	Pentadbir Sistem ICT, Warga Kementerian, Pihak Ketiga, Pakar Runding dan Pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian

A.8.7 Pertimbangan Tentang Audit Sistem Maklumat	
Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.	
A.8.7.1 Kawalan Audit Sistem Maklumat	**Peranan**
Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas penyampaian perkhidmatan.	ICTSO dan Pentadbir Sistem ICT
A.8.8 Perisikan Ancaman (*Threat Intelligent*)	
Objektif: Memberikan kesedaran berkenaan Perisikan Ancaman yang boleh mendatangkan impak atau mengancam organisasi supaya organisasi boleh mengambil tindakan atau langkah mitigasi yang sewajarnya.	
A.8.8.1 Pelaksanaan Aktiviti Perisikan Ancaman	**Peranan**
Maklumat berkaitan ancaman keselamatan maklumat hendaklah dikumpul dan dianalisis bagi kegunaan perisikan ancaman. Laporan maklumat ini adalah untuk memberikan kesedaran tentang persekitaran ancaman yang boleh memberikan kesan kepada organisasi dan tindakan mitigasi sesuai yang boleh dilaksanakan. Pelaksanaan aktiviti perisikan ancaman akan membolehkan ancaman yang mampu merosakkan organisasi dapat dielakkan atau impak sesuatu ancaman dikurangkan.	Pentadbir Sistem ICT Pentadbir Pusat Data Pentadbir Rangkaian

BIDANG A.9 : KESELAMATAN KOMUNIKASI

A.9.1 Pengurusan Keselamatan Rangkaian	
Objektif: Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.	
A.9.1.1 Kawalan Rangkaian	**Peranan**
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti yang 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 *Final Acceptance Test* (FAT) semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian; (f) Semua trafik keluar dan masuk bagi rangkaian pengguna hendaklah melalui *firewall* di bawah kawalan Kementerian; (g) Manakala semua trafik keluar dan masuk bagi rangkaian pusat data, *server* dan aplikasi milik Kementerian hendaklah melalui *firewall* di bawah kawalan Kementerian; (h) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada ICTSO;	ICTSO dan Pentadbir Sistem ICT

(i) Mengaktifkan perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat Kementerian; (j) Menggunakan kemudahan *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (k) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (l) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja.	
A.9.1.2 Keselamatan Perkhidmatan Rangkaian	**Peranan**
Pengurusan bagi semua perkhidmatan rangkaian (dalaman atau luaran) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga
A.9.1.3 Pengasingan Dalam Rangkaian	**Peranan**
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dengan Pusat Data, *server* dan aplikasi mengikut segmen rangkaian Kementerian.	ICTSO dan Pentadbir Sistem ICT
A.9.2 Pemindahan Data dan Maklumat	
Objektif: Memastikan keselamatan perpindahan/pertukaran data maklumat dan perisian antara Kementerian dan pihak luar terjamin.	
A.9.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat	**Peranan**
Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk	Pengguna, Warga Kementerian dan Agensi Luar

melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Media yang mengandungi maklumat perlu dilindungi; dan (c) Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	
A.9.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat	**Peranan**
Kementerian perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara Kementerian dengan pihak luar. Perkara yang perlu dipertimbangkan ialah: (a) CDO, SUB, KU dan Pengarah hendaklah mengawal penghantaran dan penerimaan maklumat Kementerian; (b) Prosedur sesuai perlu dikuatkuasakan bagi memastikan terdapat kawalan semasa pemindahan data dan maklumat Kementerian; (c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan (d) Kementerian hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	CDO dan SUB/KU/Pengarah
A.9.2.3 Pesanan Elektronik	**Peranan**
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.	Warga Kementerian

A.9.2.4 Perjanjian Kerahsiaan atau Ketakdedahan	**Peranan**
Syarat-syarat perjanjian kerahsiaan atau ketakdedahan (*non-disclosure*) perlu mengambil kira keperluan organisasi dan hendaklah disemak dan didokumenkan. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	ICTSO dan Pihak Ketiga

BIDANG A.10 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

A.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.	
A.10.1.1 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat	**Peranan**
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, latihan, 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 Polisi Keselamatan Siber Kementerian; (c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan (d) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem. (e) Perkhidmatan sumber luaran (*outsource*) hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala atau mengikut keperluan. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk	Pentadbir Sistem ICT

menyokong operasi Kementerian. Perkhidmatan sumber luaran merangkumi: i. Perisian Sebagai Satu Perkhidmatan / *Software as a Service* (SaaS); ii. Platform Sebagai Satu Perkhidmatan / *Platform as a Service* (PaaS); iii. Infrastruktur Sebagai Satu Perkhidmatan / *Infrastucture as a Service* (IaaS); iv. Storan Pengkomputeran Awan / *Storage as a Service* (STaaS); dan v. Pemantauan Keselamatan.	
A.10.1.2 Melindungi Perkhidmatan Aplikasi Dalam Rangkaian Awam	**Peranan**
Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala atau mengikut keperluan; (b) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*); (c) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; (d) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan (e) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	Pentadbir Sistem ICT dan Pentadbir Rangkaian

A.10.1.3 Melindungi Transaksi Perkhidmatan Aplikasi	Peranan
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 dengan transaksi; (b) Memastikan semua aspek transaksi berikut 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.	ICTSO, SUB/KU/Pengarah dan Pentadbir Sistem ICT
A.10.2 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.	
A.10.2.1 Prosedur Kawalan Perubahan Sistem	**Peranan**
Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod, didokumen dan disahkan sebelum digunakan; (b) Sistem maklumat dan aplikasi perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi	SUB/KU/Pengarah dan Pentadbir Sistem ICT

dan keselamatan organisasi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan (d) Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	
A.10.2.2 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi	**Peranan**
Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; (b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan (c) Memastikan perubahan yang sesuai dibuat kepada DRTP dan DRMP Kementerian.	Pentadbir Sistem ICT dan Pentadbir Pusat Data
A.10.2.3 Sekatan Perubahan Pakej Perisian Pihak Ketiga	**Peranan**
Pengubahsuaian ke atas pakej perisian pihak ketiga adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem ICT dan SUB/KU/Pengarah
A.10.2.4 Prinsip Kejuruteraan Sistem yang Selamat	**Peranan**
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur	Pentadbir Sistem ICT dan SUB/KU/Pengarah

kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini.	
A.10.2.5 Pengaturcaraan Selamat (*Secure Coding*)	**Peranan**
Prinsip pengekodan selamat hendaklah diwujudkan, dikemaskini dan pelaksanaannya diuji pada sistem aplikasi bagi mengurangkan risiko kelemahan sistem aplikasi yang dibangunkan. Pengaturcaraan selamat hendaklah mengikut amalan terbaik yang terdapat di dalam industri pengaturcaraan komputer.	Pentadbir Sistem ICT
A.10.2.6 Persekitaran Pembangunan Selamat	**Peranan**
Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. Kementerian perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: (a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; (b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; (c) Keperluan dalam pengasingan di arıtara pelbagai persekitaran pembangunan sistem; (d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; (e) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang orang boleh dipercayai; dan	Pentadbir Sistem ICT dan SUB/KU/Pengarah

(f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	
A.10.2.7 Pembangunan Secara Sumber Luaran (*Out Source*)	**Peranan**
Kementerian hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (*source code*) adalah menjadi hak milik Kementerian. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Kod sumber pembangunan sistem aplikasi adalah hak milik Kementerian termasuk pemilikan harta intelek sistem berkaitan; (b) Bagi pembangunan secara *customize off the shelf*, kod sumber asal adalah hak milik pembekal perkhidmatan namun kod sumber yang telah diubahsuai adalah hak milik Kementerian termasuk pemilikan harta intelek sistem berkaitan; (c) Ikatan kontrak atau perjanjian perlu dimeterai antara pihak ketiga dengan Kementerian bagi memenuhi keperluan reka bentuk selamat pembangunan sistem aplikasi berkaitan mengikut amalan terbaik; (d) Menggunapakai prinsip dan tatacara *escrow*; (e) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; dan (f) Kontrak hendaklah dipastikan boleh dibaca, difahami dan diolah semula mengikut keperluan.	Pentadbir Sistem ICT, SUB/KU/Pengarah dan ICTSO
A.10.2.8 Pengujian Keselamatan Sistem	**Peranan**
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut:	Pentadbir Sistem ICT dan ICTSO

(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 (c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	
A.10.2.9 Pengujian Penerimaan Sistem	**Peranan**
Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem aplikasi yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Pengujian penerimaan sistem hendaklah merangkumi keperluan keselamatan sistem maklumat dan mematuhi garis panduan keselamatan yang berkuatkuasa; (b) Penerimaan pengujian semua sistem aplikasi baharu dan penambahbaikan sistem aplikasi hendaklah memenuhi kriteria yang ditetapkan sebelum ia digunakan; (c) Pengujian semua sistem aplikasi baharu boleh menggunakan alat pengimbas kerentanan automatik yang digunakan untuk Ujian Imbasan Kerentanan (*vulnerability scanner*); dan (d) Penerimaan pengujian adalah berdasarkan kepada kualiti dan ketepatan serahan sistem.	Pengguna, Pentadbir Sistem ICT dan ICTSO
A.10.3 Data Ujian	
Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian.	

A.10.3.1 Perlindungan Data Ujian	**Peranan**
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; (b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan 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.	Pengguna, Pentadbir Sistem ICT dan ICTSO

BIDANG A.11 : HUBUNGAN DENGAN PEMBEKAL

A.11.1 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	
Objektif: Memastikan aset ICT Kementerian yang boleh dicapai oleh pembekal dilindungi.	
A.11.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Dengan Pembekal	**Peranan**
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset Kementerian. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori; (b) Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal; (c) Mengawal dan memantau akses pembekal; (d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; (e) Jenis-jenis obligasi kepada pembekal; (f) Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; (g) Melaksanakan program kesedaran mengenai Polisi Keselamatan Siber kepada pembekal; (h) Memastikan pembekal menandatangani Borang Pematuhan *Non Disclosure Agreement* (NDA) seperti di **LAMPIRAN B**; dan (i) Pembekal perlu mematuhi Arahan Keselamatan yang berkuatkuasa.	SUB/KU/Pengarah, Pemilik Projek dan Pembekal

A.11.1.2 Menangani Keselamatan Dalam Perjanjian Dengan Pembekal	Peranan
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. Pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak Kementerian selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Kementerian hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; (b) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; (c) Semua wakil pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; (d) Produk atau perkhidmatan yang ditawarkan oleh pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; (e) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh pembekal;	Pembekal

(f) Laporan penilaian pihak ketiga yang dikemukakan oleh pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: i. Badan penilai pihak ketiga adalah bebas dan berintegriti; ii. Badan penilai pihak ketiga adalah kompeten; iii. Kriteria penilaian; iv. Parameter pengujian; dan v. Andaian yang dibuat berkaitan dengan skop penilaian; (g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan Kementerian; dan (h) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh Kementerian.	
A.11.1.3 Rantaian Bekalan Teknologi Maklumat dan Komunikasi	**Peranan**
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan	SUB/KU/Pengarah, Pembekal dan Pemilik Projek

(c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	
A.11.2 Pengurusan Penyampaian Perkhidmatan Pembekal	
Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.	
A.11.2.1 Memantau dan Mengkaji Semula Perkhidmatan Pembekal	**Peranan**
Kementerian hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: (a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; (b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan (c) Memaklumkan mengenai insiden kesetamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	SUB/KU/Pengarah, Pembekal dan Pemilik Projek
A.11.2.2 Menguruskan Perubahan Kepada Perkhidmatan Pembekal	**Peranan**
Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut: (a) Perubahan dalam perjanjian dengan pembekal; tertakluk kepada kelulusan Lembaga Perolehan Sebutharga atau Lembaga Perolehan Tender;	SUB/KU/Pengarah, Pembekal dan Pemilik Projek

(b) Perubahan yang dilakukan oleh Kementerian bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan (c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	
A.11.3 Kawalan Penggunaan Perkhidmatan Pengkomputeran Awan (*Cloud*)	
Objektif: Mengurus dan menentukan keselamatan maklumat untuk kegunaan perkhidmatan pengkomputeran awan.	
A.11.3.1 Keselamatan Maklumat Untuk Penggunaan Perkhidmatan Pengkomputeran Awan (*Cloud*)	**Peranan**
Kementerian hendaklah memastikan keselamatan maklumat kerajaan adalah terjamin sebelum, semasa dan selepas penggunaan perkhidmatan pengkomputeran awan dengan mengambil kira perkara di bawah: (a) Memastikan bahawa penilaian risiko dilaksanakan sebelum, semasa dan selepas menggunakan perkhidmatan pengkomputeran awan; (b) Mendokumentasikan dengan jelas tanggungjawab dan peranan pembekal perkhidmatan pengkomputeran awan serta Kementerian; (c) Memastikan perjanjian yang jelas di antara pembekal perkhidmatan pengkomputeran awan dan Kerajaan. Perjanjian tersebut hendaklah mengandungi perkara di bawah: i. Pembekal hendaklah mempunyai pensijilan keselamatan yang berkaitan; ii. Pembekal hendaklah menyediakan mekanisme kawalan akses yang memenuhi keperluan	Pemilik Projek, Pentadbir Pusat Data

Kementerian; dan iii. Pembekal hendaklah menyediakan perisian bagi melindungi keselamatan maklumat daripada perisian hasad.	

BIDANG A.12 : PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

A.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.	
A.12.1.1 Tanggungjawab dan Prosedur	**Peranan**
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan siber. Pengurusan insiden Kementerian adalah berdasarkan kepada Pekeliling Am Bilangan 4 Tahun 2022, Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Memberikan kesedaran berkaitan pengurusan dan pengendalian insiden keselamatan siber dan hebahan kepada warga Kementerian; dan (b) Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.	ICTSO, SUB, CSIRT Kementerian dan Pemilik Projek
A.12.1.2 Pelaporan Kejadian Keselamatan Maklumat	**Peranan**
Insiden keselamatan siber hendaklah dilaporkan kepada CSIRT Kementerian dan NACSA dengan kadar segera melalui tatacara semasa Pelaporan Insiden NACSA. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Insiden keselamatan siber yang memberikan impak tinggi terhadap pertahanan dan keselamatan negara, kestabilan ekonomi, imej, keupayaan Kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu; (b) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa;	ICTSO, SUB dan CSIRT Kementerian

(c) Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa; (d) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (e) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; (f) Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; (g) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; (h) Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka; dan (i) Prosedur pelaporan insiden keselamatan siber berdasarkan pekeliling berkaitan yang berkuatkuasa.	
A.12.1.3 Pelaporan Kelemahan Keselamatan Maklumat	**Peranan**
Warga Kementerian dan pembekal yang menggunakan sistem dan perkhidmatan maklumat Kementerian dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.	Warga Kementerian, Pihak Ketiga, Pakar Runding dan Pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian
A.12.1.4 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat	**Peranan**
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO

A.12.1.5 Tindak Balas Terhadap Insiden Keselamatan Maklumat	**Peranan**
Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT Kementerian. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: (a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; (b) Menjalankan kajian forensik sekiranya perlu; (c) Menghubungi pihak yang berkenaan dengan secepat mungkin; (d) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; (e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (f) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; (g) Menyediakan tindakan pemulihan segera; dan (h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	ICTSO dan CSIRT Kementerian

A.12.1.6 Pembelajaran Daripada Insiden Keselamatan Maklumat	**Peranan**
Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	ICTSO dan CSIRT Kementerian
A.12.1.7 Pengumpulan Bahan Bukti	**Peranan**
Kementerian hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	ICTSO dan CSIRT Kementerian

BIDANG A.13 : ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

A.13.1 Kesinambungan Keselamatan Maklumat	
Objektif: Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan bisnes Kementerian.	
A.13.1.1 Perancangan Kesinambungan Keselamatan Maklumat	**Peranan**
Kementerian hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, Kementerian perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi Kementerian. Kementerian juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) Kementerian. (b) Menetapkan polisi PKP; (c) Mengenal pasti perkhidmatan kritikal; (d) Melaksanakan Kajian Impak Perkhidmatan (*Business Impact Analysis* - BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; (e) Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana ICT; (f) Melaksanakan program kesedaran dan latihan pasukan PKP dan warga Kementerian; (g) Melaksanakan simulasi; dan	Koordinator PKP, Pasukan ERT, CCT dan DRT

(h) Melaksanakan penyelenggaraan ke atas pelan PKP dan mengemaskini dokumen.	
A.13.1.2 Pelaksanaan Kesinambungan Keselamatan Maklumat	**Peranan**
Kementerian hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Melaksanakan *post-mortem* dan mengemaskini DRTP dan DRMP; (b) Mengemas kini DRTP dan DRMP jika berlaku perubahan kepada fungsi kritikal Kementerian; (c) Mengemas kini struktur tadbir urus DRTP dan DRMP Kementerian jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan (d) Memastikan pasukan DRTP dan DRMP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana DRTP dan DRMP.	Pasukan DRT
A.13.1.3 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat	**Peranan**
Kementerian hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa yang ditetapkan bagi memastikannya sah dan berkesan semasa situasi kecemasan.	Pengurusan Atasan Koordinator PKP, ERT, CCT, DRT, Pemilik Perkhidmatan Kritkal Kementerian dalam PKP dan Warga Kementerian

A.13.2 Lewahan (*Redundancy*)	
Objektif: Memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.	
A.13.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat	**Peranan**
Kemudahan pemprosesan maklumat Kementerian perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (*failover test)* keberkesanannya dari semasa ke semasa.	Pentadbir Pusat Data, Pemilik Perkhidmatan dan Pentadbir Sistem ICT
A.13.3 Kesinambungan Operasi	
Objektif: Memastikan ketersediaan maklumat organisasi dan aset lain yang berkaitan sekiranya berlaku gangguan.	
A.13.3.1 Ketersediaan ICT untuk Kesinambungan Operasi	**Peranan**
Kementerian hendaklah menyediakan, mendokumenkan, melaksanakan, menyelenggara dan menguji proses, prosedur dan kawalan berkaitan ICT bagi memastikan ketersediaan maklumat serta aset ICT sekiranya berlaku bencana atau gangguan. Kementerian hendaklah melaksanakan perkara berikut: (a) Memastikan Kementerian menyediakan keperluan sumber manusia yang mencukupi; mewujudkan struktur tadbir urus beserta peranan dan tanggungjawab berkaitan ICT; (b) Memastikan pasukan DRMP dan DRTP mempunyai tahap kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksanakan DRMP dan DRTP; (c) Mewujudkan dan mengemas kini DRMP dan DRTP jika berlaku perubahan seperti fungsi kritikal, pertukaran pegawai dan penambahbaikan berdasarkan keputusan pengujian; dan (d) Melaksanakan pengujian DRMP dan DRTP secara berkala berdasarkan objektif Kementerian.	Pentadbir Pusat Data, Pentadbir Sistem, Pentadbir Rangkaian dan JDN

BIDANG A.14 : PEMATUHAN

A.14.1 Pematuhan Terhadap Keperluan Perundangan dan Kontrak	
Objektif: Meningkat dan memantapkan tahap keselamatan siber bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	
A.14.1.1 Pengenalpastian Keperluan Undang-Undang dan Kontrak yang Terpakai	**Peranan**
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga Kementerian, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian. Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi adalah seperti **LAMPIRAN A.**	Warga Kementerian, Pihak Ketiga dan Pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian
A.14.1.2 Hak Harta Intelek	**Peranan**
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Warga Kementerian, Pihak Ketiga dan Pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian
A.14.1.3 Perlindungan Rekod	**Peranan**
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pernalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Warga Kementerian, Pihak Ketiga dan Pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian

A.14.1.4 Privasi dan Perlindungan Maklumat Peribadi	Peranan
Kementerian hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Warga Kementerian, Pihak Ketiga dan Pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian
A.14.2 Kajian Semula Keselamatan Maklumat	
Objektif: Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur Kementerian.	
A.14.2.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali	**Peranan**
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	SUB/KU/Pengarah dan Pemilik Projek
A.14.2.2 Pematuhan Polisi dan Standard Keselamatan	**Peranan**
Kementerian hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.	SUB/KU/Pengarah, dan Pemilik Projek
A.14.2.3 Kajian Semula Pematuhan Teknikal	**Peranan**
Kementerian hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.	SUB/KU/Pengarah, dan Pemilik Projek

LAMPIRAN A

UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Polisi Keselamatan Siber MOSTI Versi 2.0 ini hendaklah dibaca bersama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan yang berkaitan serta sedang berkuatkuasa antaranya seperti berikut:

1. Piawaian standard ISO/IEC 27001: 2022;
2. Piawaian standard ISO/IEC 27001: 2013;
3. Arahan Keselamatan;
4. Pekeliling Am Bilangan 4 Tahun 2022 bertajuk “Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam”;
5. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";
6. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002;
7. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
8. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi Agensi Kerajaan";
9. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
10. Surat Pekeliling Am Bil. 4 Tahun 2022 - "Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam";
11. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama) - "Tatacara Penyediaan, Penilaian dan PenerimaanTender';
12. Surat Pekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan";
13. Akta Tandatangan Digital 1997;
14. Akta Rahsia Rasmi 1972;
15. Akta Jenayah Komputer 1997;

16. Akta Hak Cipta (Pindaan) Tahun 1997;

17. Akta Komunikasi dan Multimedia 1998;

18. Perintah-Perintah Am;

19. Arahan Perbendaharaan;

20. Arahan Teknologi Maklumat 2007;

21. *Standard Operating Procedure* (SOP) ICT MOSTI;

22. Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";

23. Etika Penggunaan E-mel dan Internet MOSTI;

24. Surat Akujanji;

25. Pelan Kesinambungan Perkhidmatan;

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

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

28. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)";

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

30. Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007";

31. Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT MAMPU;

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

33. Garis Panduan GPKI; dan

34. 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).

LAMPIRAN B

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

NON DISCLOSURE AGREEMENT (NDA)

Saya .....

No. Kad Pengenalan ..... berjawatan .....

dari organisasi .....

dengan ini :

a) Akan memberi perlindungan kerahsiaan yang sewajarnya kepada semua maklumat dalam dokumen terbuka dan terperingkat MOSTI selaras dengan peruntukan Akta Rahsia Rasmi 1972; dan

b) Tidak mempunyai kepentingan peribadi terhadap maklumat tersebut yang saya perolehi semasa terlibat dengan .....
.....
.....

Sekian, terima kasih.

.....	.....
(Tandatangan)	(Tandatangan Saksi)
.....	.....
(Nama)	(Nama Saksi)
.....	.....
(No. Kad Pengenalan)	(No. Kad Pengenalan Saksi)
Tarikh :	Tarikh : .....

Nota : Sila isi dengan pen dakwat hitam

BAHAGIAN PENGURUSAN TEKNOLOGI MAKLUMAT
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
Aras 1, Blok C5, Kompleks C, Pusat Pentadbiran Kerajaan Persekutuan 62662 Putrajaya, Malaysia
No. Tel.: (603)-8885 8000 No. Faks: (603)-8889 3005
E-mel: enquiry@mosti.gov.my