KEMENTERIAN
PERPADUAN NEGARA

POLISI KESELAMATAN SIBER

VERSI 1.0

Diterbitkan oleh:
Kementerian Perpaduan negara
Blok F9, Parcel F,
Pusat Pentadbiran Kerajaan Persekutuan,
62000 Wilayah Persekutuan Putrajaya
Telefon : +603 - 8091 8000
Faks : +603 - 8889 4821
Laman Web : www.perpaduan.gov.my

MAKLUMAT DOKUMEN

Tajuk	**:**	**Polisi Keselamatan Siber (PKS)**
Versi	**:**	**1.0**
Tarikh Kuat Kuasa	**:**	
Pemilik	**:**	**Kementerian Perpaduan Negara**

PERUTUSAN

YBHG. DATUK KETUA SETIAUSAHA KEMENTERIAN PERPADUAN NEGARA

Assalamualaikum WBT dan Salam Perpaduan,

Terlebih dahulu saya ingin mengucapkan tahniah kepada Bahagian Pengurusan Maklumat (BPM) dan pegawai-pegawai ICT di jabatan/agensi di atas kejayaan menghasilkan Polisi Keselamatan Siber (PKS) KPN untuk dijadikan rujukan khasnya oleh warga kementerian ini.

Adalah menjadi hasrat kerajaan untuk meningkatkan keberkesanan sistem penyampaian perkhidmatan ICT melalui infrastruktur yang berteknologi dan sistem maklumat secara E*nd-to-End* (E2E). Kemajuan teknologi ICT yang begitu pesat berkembang kini sangat memberi kesan kepada sistem penyampaian perkhidmatan kerajaan. Bagi menyokong inisiatif pendigitalan sektor awam, adalah penting untuk kita selaku pengguna ICT memahami dan mengetahui kaedah serta prosedur tertentu dalam menggunakan aplikasi ICT secara berhemah yang seterusnya dapat mengurangkan risiko daripada terdedah kepada pelbagai bentuk ancaman serangan siber.

Penerbitan polisi ini akan menjadi rujukan kepada semua warga kementerian dalam pengurusan dan pelaksanaan ICT yang berkaitan dengan isu-isu keselamatan perkakasan, perisian dan juga maklumat. Justeru itu, dengan adanya polisi ini maka setiap pengguna ICT di kementerian perlu memastikan peraturan keselamatan ICT dipatuhi selaras dengan dokumen PKS ini. Pematuhan kepada PKS adalah wajib dan sebarang ketidakpatuhan dan penyelewengan boleh menyebabkan seseorang pegawai atau kakitangan diambil tindakan yang sewajarnya.

Oleh itu saya menyeru kepada semua warga KPN agar mematuhi garis panduan yang terkandung di dalam PKS bagi memastikan perkhidmatan yang disediakan oleh kementerian berjaya mencapai matlamat dan selamat daripada sebarang insiden keselamatan ICT.

Sekian, terima kasih.

YBHG DATUK WAN SURAYA BINTI WAN MOHD RADZI

PERUTUSAN

KETUA PEGAWAI MAKLUMAT
KEMENTERIAN PERPADUAN NEGARA

Assalamualaikum WBT dan Salam Perpaduan,

Syukur dipanjatkan kepada Allah SWT kerana Polisi Keselamatan Siber (PKS) Kementerian Perpaduan Negara (KPN) telah berjaya dibangunkan. Saya mengucapkan tahniah dan terima kasih kepada Bahagian Pengurusan Maklumat KPN dan pegawai-pegawai ICT agensi-agensi di bawah KPN yang telah menyumbang idea, masa dan tenaga dalam membangunkan PKS KPN ini. Walaupun KPN merupakan kementerian yang baharu, PKS KPN ini telah dibangunkan dengan teliti berpandukan kepada Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) yang telah dikeluarkan oleh pihak *National Cyber Security Agency* (NACSA) dan Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan yang telah dikeluarkan oleh pihak MAMPU.

PKS KPN adalah sangat penting kerana ia menggariskan set peraturan keselamatan siber dan mengandungi kod kelakuan yang perlu dipatuhi oleh semua pegawai KPN semasa menggunakan aset ICT dan semasa membuat capaian kepada sistem maklumat KPN. Ia merangkumi pengurusan keselamatan ke atas data, sistem, perisian, peralatan, rangkaian dan perkhidmatan ICT secara keseluruhan. Keselamatan siber perlu diberikan perhatian serius oleh semua pegawai kerana peningkatan keupayaan digital turut meningkatkan risiko keselamatan siber terhadap maklumat dan aset ICT kerajaan.

PKS KPN ini adalah terpakai untuk semua pegawai di KPN dan juga semua pegawai di agensi-agensi di bawah KPN. Saya berharap dengan adanya PKS KPN ini, semua pegawai sentiasa mematuhi peraturan keselamatan ICT yang telah ditetapkan. Pematuhan kepada PKS KPN adalah untuk memastikan tiada sebarang insiden siber berlaku yang boleh menjejaskan kesinambungan operasi perkhidmatan KPN kepada rakyat.

Sekian, terima kasih.

ZAHARIAH BINTI MOHD SARIF

SEJARAH SEMAKAN DAN PINDAAN DOKUMEN PKS

VERSI	TARIKH	RINGKASAN SEMAKAN/PINDAAN	KELULUSAN	TARIKH KUATKUASA
1.0				

SINGKATAN DAN TAKRIFAN

(1)	BCM	*Business Continuity Management*
(2)	BCP	*Business Continuity Plan*
(3)	BKP	Bahagian Khidmat Pengurusan
(4)	BPM	Bahagian Pengurusan Maklumat
(5)	CCP	*Communication Crisis Plan* / *Pelan Krisis Komunikasi*
(6)	CERT	*Computer Emergency Response Team*
(7)	CIO	*Chief Information Officer*
(8)	CGSO	*Chief Government Security Office* / Pejabat Ketua Pengawal Keselamatan Kerajaan
(9)	CNII	*Critical National Information Infrastructure* / Prasarana Maklumat Kritikal Negara
(10)	DDOS	*Distributed Denial of Service*
(11)	DRP	*Disaster Recover Plan* / Pelan Pemulihan Bencana
(12)	DRC	*Disaster Recovery Centre* / Pelan Pengurusan Pusat
(13)	ERP	*Emergency Response Planning* / Pengurusan Tindakbalas Kecemasan
(14)	GCERT	*Government Computer Emergency Response Team*
(15)	ICT	*Information and Communication Technology*
(16)	ICTSO	*ICT Security Officer*
(17)	ID	*Identity*
(18)	IDS	*Intrusion Detection System*
(19)	IPS	*Intrusion Prevention System*
(20)	ISMP	*Information System Management Planning* / Pelan Pengurusan Keselamatan Maklumat

(21)	ISMS	*Information Security Management System* / Sistem Pengurusan Keselamatan Maklumat
(22)	JTICT	Jawatankuasa Teknikal ICT
(23)	JPICT	Jawatankuasa Pemandu ICT
(24)	JKICT	Jawatankuasa Keselamatan ICT
(25)	KSU	Ketua Setiausaha
(26)	KP	Ketua Pengarah
(27)	LAN	*Local Area Network*
(28)	MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
(29)	MyCERT	*Malaysia Computer Emergency Response Team*
(30)	KPN	Kementerian Perpaduan Negara
(31)	PKI	*Public-Key Infrastructure*
(32)	PKS	Polisi Keselamatan Siber
(33)	PUU	Penasihat Undang-Undang
(34)	SMS	*Short Message Service*
(35)	SPA	Sistem Pengurusan Aset
(36)	SSM	Seksyen Sumber Manusia
(37)	UI	Unit Integriti
(38)	UPS	*Uninterruptible Power Supply*
(39)	VPN	*Virtual Private Network*
(40)	WAN	*Wide Area Network*

DEFINISI

(1)	Ketua Jabatan	Pegawai yang mengetuai sesebuah agensi awam di peringkat ibu pejabat, termasuk Ketua Setiausaha dan Ketua Pengarah.
(2)	Pegawai KPN	Pegawai yang dilantik secara tetap, kontrak, sementara dalam skim perkhidmatan.
(3)	Pegawai Aset	Pegawai yang dilantik oleh Ketua Jabatan
(4)	Pihak Ketiga	Kementerian/Jabatan/Agensi selain dari KPN, orang awam, pembekal, kontraktor yang berurusan dengan KPN
(5)	Pemilik Sistem	Bahagian/Unit/individu yang memiliki sistem
(6)	Pemilik Projek	Bahagian/Unit/individu yang mengendalikan projek
(7)	Pentadbir Rangkaian	Mengurus dan menyelia perkhidmatan rangkaian kementerian
(8)	Pentadbir Sistem	Menyelesaikan masalah sistem
(9)	Pentadbir Pusat Data	Mengurus dan menyelia pusat data kementerian
(10)	Pentadbir Aset	Mengurus dan menyelia peralatan ICT
(11)	Pengurus ICT	Pegawai yang mengurus ICT di Kementerian/Jabatan
(12)	Pengurus Sumber Manusia	Pegawai yang mengurus hal ehwal sumber manusia di KPN/Jabatan/Agensi
(13)	Pegawai Keselamatan	Pegawai yang bertanggungjawab keatas semua aspek keselamatan dokumen dan maklumat rasmi Jabatan, bangunan dan harta benda Kerajaan

PENGENALAN

Polisi Keselamatan Siber (PKS) Kementerian Perpaduan Negara (KPN) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi semasa menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Polisi ini juga menerangkan kepada pengguna mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT KPN.

OBJEKTIF

PKS KPN diwujudkan untuk menjamin kesinambungan perkhidmatan KPN dengan meminimumkan kesan insiden keselamatan ICT. Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat yang sesuai dengan perkhidmatan KPN. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi dengan baik.
Objektif utama PKS KPN diwujudkan ialah seperti berikut:

a) Memastikan kelancaran perkhidmatan KPN dengan meminimumkan kerosakan atau kemusnahan;
b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kegagalan atau kelemahan kerahsiaan, integriti, ketersediaan, kesahihan maklumat dan komunikasi;
c) Mencegah salah guna atau kecurian aset ICT Kerajaan;
d) Meminimumkan kos pemulihan ICT akibat insiden ICT; dan
e) Memperkukuhkan pengurusan keselamatan ICT KPN.

PERNYATAAN POLISI

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Pengurusan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan bebas daripada ancaman dan kelemahan yang sentiasa berubah. Keselamatan ICT bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa sebarang gangguan yang boleh menjejaskan perkhidmatan.

Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a) Melindungi maklumat rahsia dan maklumat kerajaan dari capaian tanpa kuasa yang sah;
b) Menjamin setiap maklumat adalah tepat dan sempurna;
c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d) Memastikan akses diberikan hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

PKS KPN merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a) KERAHSIAAN (*CONFIDENTIALITY*)
Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

b) INTEGRITI (*INTEGRITY*)
Data dan maklumat hendaklah tepat dan hanya boleh diubah dengan cara yang dibenarkan;

c) KETERSEDIAAN (*AVAILABILITY*)
Data dan maklumat hendaklah boleh diakses pada bila-bila masa;

d) KESAHAN (*AUTHENTICITY*)
Data dan maklumat hendaklah dijamin kesahihannya;

e) TIDAK BOLEH DISANGKAL (*NON-REPUDIATION*)
Data dan maklumat hendaklah dari punca yang tidak boleh disangkal; dan

f) KEBOLEHPERCAYAAN (***ACCOUNTABILITY*)**
Data dan maklumat hendaklah dijamin kebolehpercayaan.

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

SKOP

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

a) Data dan maklumat hendaklah boleh dicapai secara berterusan dengan cepat, tepat, mudah dan dengan cara yang diyakini selamat bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta melindungi kepentingan kementerian, perkhidmatan dan masyarakat.

Bagi memastikan keselamatan aset ICT yang berterusan, PKS KPN merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan, dalam penghantaran dan yang dibuat salinan keselamatan. Setiap aset ICT perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran keselamatan. Ini dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian aset KPN seperti berikut:

i. **Perkakasan**: Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KPN. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

ii. **Perisian**: Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian,

sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada KPN;

iii. **Perkhidmatan**: Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya;

iv. **Data dan Maklumat**: Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif KPN;

v. **Manusia**: Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian KPN bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

vi. **Premis komputer dan komunikasi**: Semua kemudahan serta premis yang diguna untuk menempatkan perkara (i) – (v) di atas.

PRINSIP-PRINSIP

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

a) **Capaian atas dasar "Perlu Tahu"**

Capaian dibenarkan dan dihadkan kepada pengguna tertentu atas dasar "perlu tahu" berdasarkan klasifikasi maklumat dan tahap tapisan keselamatan pengguna;

b) **Hak Capaian Minimum**

Hak capaian kepada pengguna dimulai pada tahap yang paling minimum. Kelulusan adalah perlu bagi membolehkan capaian pada tahap yang lebih tinggi;

c) **Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT. Tanggungjawab itu perlu dinyatakan dengan jelas dan sesuai dengan tahap sensitiviti sesuatu sumber ICT;

d) Pengasingan

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

e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, segala aset ICT hendaklah ditentukan dapat menjana dan menyimpan log keselamatan dan jejak audit;

f) Pematuhan

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

g) Pemulihan

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

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 mekanisma keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

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

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

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

KPN bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. KPN perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

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

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

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

BAB 1: PELAKSANAAN POLISI

Objektif : Memastikan hala tuju pengurusan perlindungan maklumat adalah selaras dengan keperluan perkhidmatan KPN dan peraturan serta undang-undang yang sedang berkuatkuasa.

Bil.	Perkara	Tanggungjawab
1.1	**Pelaksanaan Polisi Keselamatan Siber KPN**	
	PKS KPN ini dilaksanakan oleh KSU dengan dibantu oleh Jawatankuasa Pemandu ICT yang terdiri daripada CIO, Pengurus ICT, ICTSO dan lain-lain pegawai yang dilantik.	KSU
1.2	**Pemakaian Polisi**	
	PKS ini terpakai kepada semua Pegawai KPN dan juga pihak ketiga yang berurusan dengan KPN.	Pegawai KPN/Pihak Ketiga
1.3	**Penyelenggaraan Polisi**	
	Polisi ini tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Setiap perubahan hendaklah mendapat pengesahan ICTSO. Perubahan yang melibatkan penambahan atau pemansuhan yang memberi impak ke atas keselamatan adalah dianggap perubahan utama dan hendaklah mendapat pengesahan JPICT KPN. Prosedur semakan semula polisi ini adalah seperti berikut: a) Menyemak sekurang-kurangnya satu (1) kali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan atau perubahan secara bertulis; dan c) Memaklumkan pindaan atau perubahan polisi yang telah dipersetujui kepada semua pegawai KPN dan Pihak Ketiga.	ICTSO

BAB 2: ORGANISASI KESELAMATAN

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

Bil.	Perkara	Tanggungjawab
2.1	**Organisasi Keselamatan Maklumat**	
2.1.1	**Peranan dan tanggungjawab Ketua Jabatan**	
	Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut: a) Melantik CIO di Kementerian/Jabatan; b) Melantik ICTSO di Kementerian/Jabatan untuk melaksanakan tugas-tugas yang melibatkan keselamatan siber; c) Memastikan semua pegawai KPN memahami dan mematuhi kandungan PKS KPN; d) Mengurus dan memantau perkara-perkara berkaitan dengan keselamatan siber; dan e) Memastikan pelaksanaan program kesedaran dan latihan keselamatan siber.	KSU/KP
2.1.2	**Ketua Pegawai Maklumat (CIO)**	
	a) Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber KPN dan semua jabatan/agensi di bawahnya; b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategi keselamatan siber KPN dan semua jabatan/agensi di bawahnya;	CIO

Bil.	Perkara	Tanggungjawab
c)	Merancang, menyelaras dan menyeragamkan pelaksanaan program/projek-projek keselamatan siber KPN dan jabatan/agensi di bawahnya supaya selaras dengan Pelan Strategik ICT KPN;	
d)	Memastikan keperluan sumber bagi keselamatan siber KPN adalah mencukupi; dan	
e)	Memastikan pelaksanaan penilaian risiko keselamatan siber KPN dan insiden keselamatan siber dilaporkan kepada pengurusan KPN.	
2.1.3	**Pegawai Keselamatan ICT (ICTSO)**	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:		ICTSO
a)	Merancang, melaksana, mengurus dan memantau program keselamatan siber KPN;	
b)	Menguatkuasakan PKS KPN;	
c)	Memberikan penerangan dan pendedahan berkenaan PKS KPN kepada pegawai KPN;	
d)	Mewujudkan garis panduan dan prosedur selaras dengan keperluan PKS KPN;	
e)	Melaksanakan pengurusan risiko keselamatan siber;	
f)	Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;	
g)	Memberi amaran kepada agensi terhadap kemungkinan berlakunya ancaman keselamatan siber seperti virus komputer dan penggodaman serta	

Bil.	Perkara	Tanggungjawab
	memberi khidmat nasihat dan bantuan teknikal bagi menyediakan langkah perlindungan yang bersesuaian;	
h)	Melaporkan insiden keselamatan siber kepada CIO;	
i)	Bekerjasama dengan semua pihak yang berkaitan dalam menangani ancaman atau insiden keselamatan siber dan memperakukan langkah penyelesaian atau pencegahan; dan	
j)	Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar PKS KPN setelah siasatan dalaman selesai dilaksanakan.	
2.1.4	**Pengurus ICT**	
Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:		Pengurus ICT
a)	Memastikan kajian semula dan pelaksanaan kawalan keselamatan siber selaras dengan keperluan KPN;	
b)	Melaporkan ancaman atau insiden keselamatan siber kepada ICTSO;	
c)	Menentukan kawalan capaian pengguna terhadap aset ICT; dan	
d)	Memastikan penyimpanan rekod, bahan bukti dan laporan ancaman atau insiden keselamatan siber KPN dilaksanakan dengan berkesan.	
2.1.5	**Pentadbir Sistem ICT**	
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:		Pentadbir Sistem ICT
a)	Menjaga kerahsiaan maklumat keselamatan siber;	

Bil.	Perkara	Tanggungjawab
b)	Mengambil tindakan segera apabila dimaklumkan mengenai sebarang perubahan dalam peranan dan tanggungjawab berkaitan perkhidmatan ICT yang melibatkan pegawai KPN/Pihak Ketiga;	
c)	Menentukan pelaksanaan tahap capaian kemudahan ICT adalah bertepatan dengan arahan pemilik sistem;	
d)	Memantau dan menyediakan laporan aktiviti penggunaan dan capaian pegawai KPN/Pihak Ketiga;	
e)	Mengenal pasti dan melaporkan aktiviti tidak normal berkaitan ICT kepada Pengurus ICT; dan	
f)	Menyimpan dan menganalisis rekod jejak audit.	
2.1.6	**Pentadbir Rangkaian ICT**	
Pentadbir Rangkaian ICT adalah berperanan dan bertanggungjawab seperti berikut:		Pentadbir Rangkaian ICT
a)	Memastikan rangkaian setempat (*LAN*), rangkaian luas (*WAN*) dan rangkaian tanpa wayar (*Wireless)* beroperasi sepanjang masa;	
b)	Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;	
c)	Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian;	
d)	Mewartakan polisi dan garis panduan penggunaan rangkaian Kementerian/Jabatan/Agensi kepada pengguna; dan	
e)	Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (*Security Posture*	

Bil.	Perkara	Tanggungjawab
	Assessment) (SPA) serta penilaian risiko keselamatan maklumat.	
2.1.7	**Pentadbir Pusat Data**	
	Pentadbir Pusat Data adalah berperanan dan bertanggungjawab seperti berikut: a) Memastikan persekitaran fizikal, data dan sistem aplikasi berada dalam keadaan baik dan selamat; b) Menjadual dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala; c) Menyediakan Pelan Pemulihan Bencana (DRP) bagi memastikan kesinambungan perkhidmatan; dan d) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan.	Pentadbir Pusat Data
2.1.8	**Pegawai Aset**	
	Pegawai Aset KPN ialah pegawai yang dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab Pegawai Aset adalah seperti berikut: a) Memastikan pengurusan peralatan ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan; b) Memastikan penerimaan peralatan ICT Kerajaan dilaksanakan oleh Pegawai Aset yang dilantik secara rasmi; c) Memastikan semua peralatan ICT yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan peralatan;	Pegawai Aset

Bil.	Perkara	Tanggungjawab
d)	Memastikan semua peralatan ICT yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Peralatan ICT tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan bertulis daripada Pegawai Aset;	
e)	Memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/penggantian/penaiktarafan aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira;	
f)	Memastikan semua peralatan ICT diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama Kementerian/Jabatan/Agensi berkenaan di tempat yang mudah dilihat dan sesuai pada peralatan ICT berkenaan;	
g)	Memastikan semua peralatan ICT ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan;	
h)	Memastikan senarai daftar induk peralatan ICT disediakan;	
i)	Memastikan senarai peralatan ICT disediakan mengikut lokasi dan format Senarai Aset ICT Kerajaan dalam dua (2) salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset dan satu (1) salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi;	
j)	Memastikan setiap kerosakan peralatan ICT dilaporkan;	

Bil.	Perkara	Tanggungjawab
k)	Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan peralatan ICT;	
l)	Merancang, memantau dan memastikan pemeriksaan peralatan ICT dilaksanakan sekurang-kurangnya satu (1) kali setahun; dan	
m)	Memastikan setiap kes kehilangan peralatan ICT dilaporkan dan diuruskan dengan teratur.	
2.1.9	**Pegawai KPN**	
	Pegawai KPN mempunyai peranan dan tanggungjawab seperti berikut:	Pegawai KPN
a)	Membaca, memahami dan mematuhi PKS KPN;	
b)	Menjaga kerahsiaan maklumat berkaitan penggunaan ICT;	
c)	Mengikuti dan menghayati program kesedaran keselamatan siber;	
d)	Melaporkan aktiviti yang tidak normal berkaitan ICT kepada Pegawai ICT Kementerian/Jabatan; dan	
e)	Menandatangani Surat Akuan Pematuhan PKS KPN seperti di **LAMPIRAN A** atau yang setara dengannya.	
2.1.10	**Pihak Ketiga**	
	Peranan dan tanggungjawab Pihak Ketiga adalah seperti berikut:	Pihak Ketiga
a)	Menjaga kerahsiaan maklumat berkaitan penggunaan ICT;	

Bil.	Perkara	Tanggungjawab
b)	Menandatangani perakuan pematuhan keselamatan siber yang ditetapkan oleh Kerajaan Malaysia atau peraturan yang setara/berkaitan yang berkuat kuasa;	
c)	Melaporkan aktiviti yang tidak normal berkaitan ICT kepada Pegawai ICT Kementerian/Jabatan; dan	
d)	Mendapatkan kelulusan untuk menggunakan kemudahan, perkhidmatan dan peralatan ICT KPN.	
2.2	**Peranti Mudah Alih dan *Teleworking***	
2.2.1	**Peranti Mudah Alih Milik Persendirian**	
Peranti mudah alih milik persendirian hendaklah mendapat kelulusan daripada ICTSO untuk mencapai maklumat Rahsia Rasmi dan wajib mematuhi polisi serta prosedur yang ditetapkan untuk dibawa masuk ke kawasan terperingkat.		ICTSO
2.2.2	***Teleworking***	
a)	Aktiviti yang melibatkan *Teleworking* hendaklah mendapatkan kelulusan daripada ICTSO;	ICTSO
b)	Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi peralatan ICT, data dan rangkaian dari risiko penggunaan peralatan mudah alih serta kemudahan komunikasi;	
c)	Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan	
d)	Memastikan bahawa *antivirus* digunakan dan sentiasa dikemaskini pada peralatan ICT yang digunakan.	

BAB 3: KESELAMATAN SUMBER MANUSIA

Objektif : Memastikan semua pihak yang terlibat dalam pengurusan dan penggunaan ICT memahami tanggungjawab dan peranan, meningkatkan pengetahuan dan kesedaran, menguruskan aspek keselamatan secara teratur bagi meningkatkan keselamatan penyampaian maklumat, mengurangkan risiko penyalahgunaan peralatan ICT dan mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

Bil.	Perkara	Tanggungjawab
3.1	**Sebelum Dalam Perkhidmatan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menjelaskan peranan dan tanggungjawab pihak yang terlibat dalam meningkatkan keselamatan penyampaian maklumat dan mengurangkan risiko penyalahgunaan peralatan ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pihak yang terlibat selaras dengan keperluan perkhidmatan, mengikut peraturan sedia ada; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani.	ICTSO/Pengurus ICT/Pengurus Sumber Manusia/Pegawai KPN/Pihak Ketiga
3.2	**Semasa Dalam Perkhidmatan**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Mewajibkan pihak terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan (*non-disclosure*) seperti Arahan Keselamatan. Salinan asal perjanjian yang	ICTSO/ Pengurus ICT/Pengurus Sumber Manusia/Pegawai KPN/Pihak Ketiga

Bil.	Perkara	Tanggungjawab

ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan;

b) Memastikan pihak yang terlibat mematuhi keselamatan siber berdasarkan kepada dasar dan peraturan yang ditetapkan oleh Kerajaan;

c) Memastikan tindakan disiplin atau undang-undang dilaksanakan sekiranya berlaku pelanggaran peraturan yang ditetapkan;

d) Memastikan tanggungjawab dan peranan dalam pengurusan keselamatan siber dinyatakan dalam senarai tugas yang merangkumi:

   i. Tanggungjawab pegawai KPN;

   ii. Hubungan dengan pengurusan atasan; dan

   iii. Tanggungjawab pegawai KPN dalam keselamatan siber.

e) Pegawai KPN hendaklah diberi latihan yang bersesuaian dan berterusan dalam semua aspek keselamatan siber yang berkaitan dengan tugasan mereka;

f) Pegawai KPN bertanggungjawab mengikuti latihan pengurusan keselamatan siber berdasarkan keperluan;

g) ICTSO bertanggungjawab mengkaji semula keperluan latihan keselamatan siber untuk setiap pegawai KPN;

h) Program kesedaran keselamatan siber juga perlu dilaksanakan secara berterusan sebagai langkah peringatan kepada pegawai KPN berkenaan kepentingan keselamatan peralatan ICT KPN; dan

Bil.	Perkara	Tanggungjawab
	i) Setiap pegawai KPN perlu mengikuti program kesedaran keselamatan siber secara berkala sekurang-kurangnya satu (1) kali setahun.	
3.3	**Bertukar/Tamat Perkhidmatan/Cuti Belajar**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua peralatan ICT dikembalikan kepada KPN mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau menarik balik semua kebenaran capaian ke atas peralatan ICT mengikut peraturan yang ditetapkan.	ICTSO/Pentadbir Sistem/Pegawai KPN/Pihak Ketiga

BAB 4: PENGURUSAN ASET

Objektif : Memastikan setiap aset hendaklah dikenal pasti, dikelas, direkod dan diselenggara untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua peralatan ICT.

Bil.	Perkara	Tanggungjawab
4.1	**Tanggungjawab Terhadap Peralatan ICT**	
4.1.1	**Inventori dan Pemilikan Peralatan ICT**	
	Semua peralatan ICT di KPN mestilah diuruskan mengikut peraturan dan tatacara yang berkuat kuasa seperti berikut: a) Setiap peralatan ICT hendaklah didaftarkan dan ditentukan pemiliknya. Pegawai Aset adalah bertanggungjawab mengenal pasti Pegawai KPN berdasarkan kelayakan; b) Pegawai KPN hendaklah menentukan tahap kerahsiaan yang bersesuaian bagi setiap maklumat yang terkandung di dalam peralatan ICT yang dimilikinya. Pegawai KPN juga hendaklah membuat keputusan dalam menentukan individu yang dibenarkan untuk capaian dan penggunaan maklumat tersebut; c) Pegawai Aset adalah bertanggungjawab untuk menentukan prosedur kawalan khas (contohnya: kawalan capaian), kaedah pelaksanaan dan penyelenggaraan serta menyediakan langkah pemulihan yang konsisten dengan arahan Pegawai KPN; d) Semua Pegawai KPN/Pihak Ketiga mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh Pegawai Aset;	Pegawai Aset/ Pegawai KPN/ Pihak Ketiga

Bil.	Perkara	Tanggungjawab
e)	Kehilangan/kecurian peralatan ICT mestilah dilaporkan serta merta mengikut prosedur pengurusan kehilangan/kecurian aset berpandukan Arahan Perbendaharaan yang telah ditetapkan;	
f)	Senarai maklumat peralatan ICT di KPN hendaklah diwujudkan dengan menerangkan dengan jelas pemilikan, lokasi semasa dan dokumentasi yang terlibat. Senarai peralatan ICT hendaklah disimpan oleh Pegawai Aset; dan	
g)	Setiap Pegawai KPN/Pihak Ketiga adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan peralatan ICT di bawah tanggungannya.	
4.1.2	**Peralatan Mudah Alih dan Kerja Jarak Jauh**	
Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti berikut:		Pegawai Aset/ Pegawai KPN/ Pihak Ketiga
a)	Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;	
b)	Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat;	
c)	Memastikan bahawa *antivirus* digunakan dan sentiasa dikemaskinikan untuk peralatan ICT;	

Bil.	Perkara	Tanggungjawab
	d) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan e) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	
4.1.3	**Peminjaman dan Pemulangan Peralatan ICT**	
	<u>Peminjaman</u> Langkah-langkah perlu diambil termasuklah seperti berikut: a) Mendapatkan kelulusan untuk membawa keluar peralatan ICT bagi tujuan yang dibenarkan mengikut peraturan yang telah ditetapkan; b) Melindungi dan mengawal peralatan ICT sepanjang masa; c) Merekodkan aktiviti peminjaman dan pemulangan peralatan ICT; dan d) Memastikan senarai peralatan ICT yang lengkap dan berfungsi ketika peminjaman dan pemulangan dilakukan. **<u>Pemulangan</u>** Memastikan semua peralatan ICT dikembalikan dalam keadaan lengkap dan berfungsi kepada KPN mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan bagi pegawai yang: a) Bertukar keluar; b) Bersara;	Pegawai Aset/ Pegawai KPN/ Pihak Ketiga

Bil.	Perkara	Tanggungjawab
	c) Ditamatkan perkhidmatan; dan d) Diarahkan oleh Ketua Jabatan. Membatalkan atau menarik balik semua kebenaran capaian ke atas peralatan ICT mengikut peraturan yang ditetapkan.	
4.2	**Pengelasan, Pelabelan dan Pengendalian Maklumat**	
4.2.1	**Pengelasan Maklumat**	
	Pengelasan maklumat bertujuan memastikan setiap maklumat diberi perlindungan oleh Pegawai KPN untuk menentukan keperluan, keutamaan dan tahap keselamatan berdasarkan peraturan yang berkuat kuasa seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; d) Terhad; dan e) Data Terbuka.	Pegawai Aset/ Pegawai KPN/ Pihak Ketiga
4.2.2	**Pelabelan dan Pengendalian Maklumat**	
	Semua maklumat mestilah dilabelkan mengikut klasifikasi maklumat seperti yang dinyatakan pada para 4.2.1 Pengelasan Maklumat. a) Aktiviti yang melibatkan pemprosesan maklumat seperti penyalinan, penyimpanan, penghantaran (sama ada dari segi lisan, pos, faksimile dan mel elektronik) dan pemusnahan maklumat mestilah mengikut standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; dan	Pegawai Aset/ Pegawai KPN/ Pihak Ketiga

Bil.	Perkara	Tanggungjawab
b)	Maklumat yang diklasifikasikan sebagai Rahsia Besar, Rahsia, Sulit dan Terhad perlu dilindungi daripada didedahkan kepada Pihak Ketiga atau awam. Pihak Ketiga jika perlu boleh diberi kebenaran capaian maklumat KPN atas dasar perlu tahu sahaja dan mestilah mendapat kebenaran daripada KPN.	
4.3	**Pengendalian Media Penyimpanan Maklumat**	
4.3.1	**Pengurusan Media**	
a)	Memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan media secara tidak sah dan yang boleh mengganggu aktiviti perkhidmatan;	Pegawai Aset/ Pegawai KPN/ Pihak Ketiga
b)	Prosedur perlu disediakan untuk pengurusan peralatan penyimpanan maklumat mudah alih;	
c)	Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna; dan	
d)	Maklumat yang terdapat dalam mel elektronik perlu dilindungi mengikut Akta Rahsia Rasmi Kerajaan.	
4.3.2	**Pelupusan Media**	
Peralatan penyimpanan maklumat yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan.		Pentadbir Aset
4.3.3	**Pemindahan Media**	
Polisi, prosedur dan kawalan pertukaran maklumat yang rasmi perlu diwujudkan untuk melindungi pertukaran		Pegawai Aset/ Pegawai KPN/ Pihak Ketiga

Bil.	Perkara	Tanggungjawab
	maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi dalam agensi dan mana-mana pihak terjamin. a) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara agensi dengan pihak luar; dan b) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari agensi.	

BAB 5: PENGURUSAN KAWALAN CAPAIAN

Objektif : Mengawal capaian ke atas maklumat, peralatan ICT, rangkaian dan sistem maklumat.

Bil.	Perkara	Tanggungjawab
5.1	**Pengurusan Kawalan Capaian**	
5.1.1	**Keperluan Kawalan Capaian**	
	Capaian 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. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan serta keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas peralatan ICT mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; d) Kawalan ke atas kemudahan had capaian maklumat; dan e) Kawalan capaian perlu dilaksanakan bersama kawalan fizikal dan persekitaran.	Pentadbir Rangkaian/ Pentadbir Sistem/ Pegawai KPN/ Pihak Ketiga

Bil.	Perkara	Tanggungjawab
5.2	**Pengurusan Capaian Pegawai KPN/Pihak Ketiga**	
5.2.1	**Akaun Pegawai KPN/Pihak Ketiga**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan; b) Akaun Pegawai KPN/Pihak Ketiga mestilah unik dan Pegawai KPN/Pihak Ketiga bertanggungjawab sepenuhnya ke atas akaun tersebut selepas pengesahan penerimaan dibuat; c) Pewujudan akaun Pegawai KPN/Pihak Ketiga dan perubahan tahap capaian mestilah mendapat kebenaran secara bertulis dan direkodkan; d) Pemilikan akaun dan capaian Pegawai KPN/Pihak Ketiga adalah tertakluk kepada peraturan KPN dan tindakan pengemaskinian dan/atau pembatalan hendaklah diambil atas sebab seperti berikut: i. Pegawai KPN/Pihak Ketiga tidak hadir bertugas tanpa kebenaran melebihi dari tujuh (7) hari; ii. Pegawai KPN/Pihak Ketiga bercuti atau bertugas di luar pejabat mengikut peraturan yang berkuat kuasa; iii. Pegawai KPN/Pihak Ketiga bertukar jawatan, tanggungjawab dan bidang tugas. Pembatalan akan dilakukan setelah dimaklumkan oleh Pengurusan Sumber Manusia (PSM); iv. Pegawai KPN/Pihak Ketiga yang sedang dalam prosiding dan/atau dikenakan tindakan tatatertib	Pentadbir Rangkaian/ Pentadbir Sistem/ Pegawai KPN/ Pihak Ketiga

Bil.	Perkara	Tanggungjawab
	oleh Pihak Berkuasa Tatatertib. Pembatalan akan dilakukan serta merta apabila dimaklumkan oleh pihak yang mengendalikan Pengurusan Sumber Manusia (PSM); dan v. Pegawai KPN/Pihak Ketiga bertukar, berpindah, bersara dan/atau tamat perkhidmatan. Pembatalan akan dilakukan berdasarkan tarikh arahan yang dikeluarkan oleh Pengurusan Sumber Manusia (PSM). e) Aktiviti capaian oleh Pegawai KPN/Pihak Ketiga direkod dan diselenggarakan dengan sistematik dari semasa ke semasa. Maklumat yang direkod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya; dan f) Akaun Pegawai KPN/Pihak Ketiga yang baru diwujudkan perlu diberikan kata laluan sementara dan Pegawai KPN/Pihak Ketiga perlu menukar kata laluan apabila log masuk dibuat pada kali pertama.	
5.2.2	**Hak Capaian**	
a)	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas; dan	Pentadbir Sistem/Pegawai KPN/Pihak Ketiga
b)	Sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan.	

Bil.	Perkara	Tanggungjawab
5.2.3	**Pengurusan Kata Laluan**	
a)	Memastikan pengunaan ID Pegawai KPN/Pihak Ketiga dan kata laluan tidak dikongsi;	Pentadbir Sistem/Pegawai KPN/Pihak Ketiga
b)	Membenarkan Pegawai KPN/Pihak Ketiga menukar kata laluan sendiri;	
c)	Menggunakan kata laluan yang berkualiti (sekurang-kurangnya dua belas (12) aksara dengan gabungan huruf, nombor dan simbol);	
d)	Mewajibkan Pegawai KPN/Pihak Ketiga menukar kata laluan apabila log masuk kali pertama;	
e)	Menyimpan rekod bagi kata laluan terdahulu dan mengelakkan penggunaan kata laluan yang berulang;	
f)	Tidak memaparkan kata laluan di skrin ketika log masuk;	
g)	Pegawai KPN/Pihak Ketiga hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;	
h)	Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun;	
i)	Menyimpan kata laluan di dalam fail yang berasingan dengan fail data aplikasi; dan	
j)	Mewajibkan Pegawai KPN/Pihak Ketiga menukar kata laluan sekurang-kurangnya setiap tiga (3) bulan untuk ke semua sistem utama.	

Bil.	Perkara	Tanggungjawab
5.3	**Kawalan Capaian Rangkaian**	
5.3.1	**Capaian Rangkaian**	
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Mewujudkan dan menguatkuasakan mekanisma untuk pengesahan identiti dan peralatan; dan b) Memantau dan menguatkuasakan kawalan capaian terhadap perkhidmatan rangkaian ICT.	ICTSO/Pentadbir Sistem/Pentadbir Rangkaian
5.3.2	**Capaian Internet**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan Internet hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian; b) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. ICTSO berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; c) Laman sesawang yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/pegawai yang diberi kuasa; d) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;	ICTSO/Pengurus ICT/Pentadbir Sistem/Pentadbir Rangkaian/ Pegawai KPN/Pihak Ketiga

Bil.	Perkara	Tanggungjawab
e)	Dokumen rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet;	
f)	Pegawai KPN/Pihak Ketiga hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; dan	
g)	Pegawai KPN/Pihak Ketiga adalah dilarang melakukan aktiviti seperti berikut:	
	i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan	
	ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah, perjudian atau keganasan.	
5.4	**Kawalan Capaian dan Sistem Maklumat**	
5.4.1	**Capaian Sistem Pengoperasian**	
a)	Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;	Pentadbir Sistem/ Pentadbir Rangkaian
b)	Mewujudkan satu akaun yang unik untuk setiap Pegawai KPN/Pihak Ketiga dan hanya digunakan oleh Pegawai KPN/Pihak Ketiga berkenaan sahaja;	
c)	Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*;	

Bil.	Perkara	Tanggungjawab
d)	Menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan	
e)	Menghadkan dan mengawal penggunaan program.	
5.4.2	**Capaian Sistem Maklumat**	
a)	Pegawai KPN/Pihak Ketiga hanya boleh menggunakan sistem maklumat yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;	Pentadbir Sistem/ Pentadbir Rangkaian/ Pegawai KPN/Pihak Ketiga
b)	Setiap capaian kepada sistem maklumat hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;	
c)	Setiap capaian kepada sistem maklumat yang berisiko tinggi hendaklah dihadkan;	
d)	Menghadkan akaun capaian sistem kepada lima (5) kali percubaan. Sekiranya gagal, akaun atau kata laluan akan disekat;	
e)	Menamatkan sesuatu sesi capaian yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan;	
f)	Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem maklumat terperingkat (sulit/rahsia);	
g)	Pegawai KPN/Pihak Ketiga digalakkan membuat enkripsi dengan menukarkan teks biasa (plain text) kepada bentuk *cipher text* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa; dan	

Bil.	Perkara	Tanggungjawab
h)	Capaian sistem dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
5.5	**Tanggungjawab Pegawai KPN/Pihak Ketiga**	
Pegawai KPN/Pihak Ketiga perlu mematuhi amalan terbaik penggunaan kata laluan seperti berikut:		Pegawai KPN/Pihak Ketiga
a)	Pegawai KPN/Pihak Ketiga tidak seharusnya menulis atau menyimpan kata laluan tanpa enkripsi di atas talian melainkan pada kes-kes tertentu di mana ia diperlukan oleh prosedur operasi seperti penyimpanan *root ID* dan kata laluan bagi sistem utama. Di dalam hal ini, kata laluan haruslah dilindungi dengan menggunakan mekanisma kawalan lain seperti menyimpan kata laluan di dalam laci berkunci dan menggunakan kata laluan yang berbeza bagi capaian berbeza;	
b)	Pegawai KPN/Pihak Ketiga adalah tidak digalakkan mengguna kata laluan yang sama bagi kegunaan sistem di KPN mahupun sistem yang tidak terdapat di KPN;	
c)	Pegawai KPN/Pihak Ketiga mestilah tidak mendedahkan kata laluan yang diguna pakai di KPN kepada sesiapa. Ini termasuklah ahli keluarga dan bukan ahli keluarga apabila melakukan kerja pejabat di rumah. Walaubagaimana pun, bagi ID kata laluan utama yang disimpan di dalam laci berkunci, harus diadakan satu proses mengenai tatacara memperoleh kata laluan berkenaan sekiranya berlaku	

Bil.	Perkara	Tanggungjawab

ketidakhadiran pemegang kata laluan utama sewaktu ia diperlukan;

d) Pegawai KPN/Pihak Ketiga haruslah menyimpan kata laluan dengan selamat dan tidak dibenarkan berkongsi akaun dengan pengguna lain. Pegawai KPN/Pihak Ketiga yang disahkan adalah bertanggungjawab ke atas kerahsiaan dan keselamatan kata laluan dan akaun mereka;

e) Penggunaan atribut *Remember Me* adalah tidak dibenarkan sama sekali. Sekiranya akaun atau kata laluan disyaki telah dicerobohi, maka laporan kejadian hendaklah dilaporkan kepada pasukan *Computer Emergency Response Team* KPN (KPN*CERT) dan tindakan menukar kata laluan perlu dilakukan;

f) Menggunakan kata laluan yang sukar diramal. Kata laluan adalah bukan perkataan di dalam mana-mana bahasa, dialek, loghat dan sebagainya. Kata laluan tidak seharusnya berdasarkan maklumat peribadi, nama ahli keluarga dan seumpamanya; dan

g) Sistem pengurusan kata laluan hendaklah menekankan pilihan kata laluan yang berkualiti. Kata laluan yang berkualiti antara lainnya mempunyai ciri-ciri seperti berikut:

   i. Gabungan minimum dua belas (12) aksara yang mengandungi kombinasi antara huruf, nombor dan simbol (seperti: 0-9, a-z, A-Z, ! @ # $ % ^ & * ( ) - +); dan

Bil.	Perkara	Tanggungjawab
	ii. Kata laluan yang ditentukan oleh Pegawai KPN/Pihak Ketiga hendaklah tidak digunakan semula. Pegawai KPN/Pihak Ketiga haruslah tidak membina kata laluan yang sama atau seakan-akan serupa seperti mana yang pernah digunakan sebelum ini di tempat lain. Khususnya, lima (5) kata laluan yang pernah digunakan sebelum ini tidak digunakan semula.	

BAB 6: KRIPTOGRAFI

Objektif : Kerahsiaan, integriti, ketersediaan, kesahan, tanpa-sangkalan dan kebolehpercayaan.

Bil.	Perkara	Tanggungjawab
6.1	**Kriptografi**	
	Kriptografi bermaksud sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja. Tindakan melindungi kerahsiaan, integriti dan ketersediaan maklumat melalui kawalan kriptografi yang boleh dilakukan adalah seperti berikut: a) Penggunaan enkripsi dengan menukarkan teks biasa (*plain text*) kepada bentuk *cipher text* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa; b) Penggunaan fungsi *hash* dan Kod Pengesahan Mesej (MAC); c) Penggunaan tandatangan digital digalakkan kepada semua Pegawai KPN/Pihak Ketiga yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; d) Pengurusan ke atas *Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut; e) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan f) Kawalan ke atas kemudahan had capaian maklumat.	Pegawai KPN/ Pihak Ketiga

BAB 7: KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif : Memastikan premis dan kemudahan ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

Bil.	Perkara	Tanggungjawab
7.1.	**Keselamatan Persekitaran**	
7.1.1.	**Keselamatan Fizikal**	
	Keselamatan fizikal adalah bertujuan untuk mengesan, menghalang dan mencegah cubaan untuk menceroboh premis. Langkah-langkah keselamatan fizikal adalah seperti berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan dan kunci harus disimpan oleh pegawai bertanggungjawab; c) Memperkukuhkan dinding dan siling; d) Memasang alat penggera dan sistem CCTV; e) Mengehadkan jalan masuk dan keluar; f) Menyediakan kaunter kawalan; g) Menyediakan tempat atau bilik khas untuk Pihak Ketiga; h) Mewujudkan perkhidmatan kawalan keselamatan; i) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan Pegawai KPN yang mendapat kebenaran sahaja untuk masuk;	CGSO/Pegawai Keselamatan/ CIO/ICTSO

Bil.	Perkara	Tanggungjawab
	j) Mereka bentuk dan melaksanakan perlindungan fizikal daripada bencana seperti kebakaran, banjir, letupan atau huru hara; k) Menyediakan garis panduan keselamatan untuk Pegawai KPN yang bekerja di dalam kawasan terhad; l) Sistem kawalan kunci dengan menetapkan Pegawai KPN yang bertanggungjawab untuk menyimpan kunci dengan baik dan mempunyai rekod; dan m) Mewujudkan kawalan di kawasan penghantaran, pemunggahan dan kawasan larangan.	
7.1.2	**Kawalan Masuk Fizikal**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap Pegawai KPN hendaklah memakai Pas Keselamatan sepanjang waktu bertugas; b) Pihak Ketiga mestilah mendaftar dan mendapatkan Pas Pelawat di pintu masuk utama KPN untuk ke kawasan/tempat berurusan dan hendaklah dikembalikan semula selepas tamat urusan; c) Semua Pas Keselamatan hendaklah diserahkan semula kepada KPN apabila pengguna bertukar, berhenti atau bersara; dan d) Kehilangan Pas Keselamatan mestilah dilaporkan dengan segera kepada Pegawai Keselamatan KPN.	Pegawai KPN/Pegawai Keselamatan/ Pihak Ketiga
7.1.3	**Kawasan Larangan**	
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam	ICTSO/Pegawai KPN/Pegawai Keselamatan

Bil.	Perkara	Tanggungjawab
	kawasan tersebut. Kawasan larangan di KPN adalah di Bilik Pusat Data, Bilik Fail dan lain-lain. a) Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja; b) Pihak Ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mendapat kebenaran untuk temujanji. Mereka hendaklah diiringi sepanjang masa sehingga tugas atau temujanji di kawasan berkenaan selesai; c) Semua aktiviti Pihak Ketiga di kawasan larangan perlu mendapat kebenaran, dipantau dan dikawal oleh Pegawai Keselamatan KPN yang bertanggungjawab; d) Peralatan komunikasi/media perakam dan media storan adalah tidak dibenarkan dibawa masuk ke dalam Pusat Data; dan e) Aktiviti mengambil gambar, merakam video, merekod suara atau penggunaan peralatan yang tidak berkenaan adalah dilarang.	Pihak Ketiga
7.2	**Keselamatan Peralatan ICT dan Maklumat**	
7.2.1	**Peralatan ICT**	
	Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan dengan mengambil tindakan berikut: a) Pegawai KPN mesti mendapat kebenaran daripada ICTSO untuk membuat instalasi perisian tambahan;	ICTSO/Pentabir Sistem/Pegawai Aset/Pegawai KPN/Pihak Ketiga

Bil.	Perkara	Tanggungjawab
b)	Pegawai KPN mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan;	
c)	Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;	
d)	Semua peralatan ICT perlu disokong oleh *Uninterruptible Power Supply* (UPS);	
e)	Semua peralatan ICT yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;	
f)	Peralatan ICT yang hendak dibawa keluar dari premis KPN untuk tujuan rasmi, perlu mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;	
g)	Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;	
h)	Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;	
i)	Pegawai KPN mesti mendapat kebenaran daripada ICTSO atau Pegawai Aset untuk mengubah kedudukan komputer dari tempat asal;	
j)	Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pegawai Aset untuk dibaik pulih;	
k)	Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan;	
l)	Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;	

Bil.	Perkara	Tanggungjawab
m)	Pegawai KPN dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem;	
n)	Pegawai KPN bertanggungjawab terhadap peralatan ICT yang digunakannya;	
o)	Pegawai KPN perlu memastikan peralatan ICT digunakan untuk urusan rasmi sahaja;	
p)	Pegawai KPN hendaklah memastikan semua peralatan ICT dalam keadaan "*OFF*" apabila meninggalkan pejabat;	
q)	Memastikan *plug* dicabut daripada suis utama (*main switch*) sebelum meninggalkan pejabat bagi mengelakkan kerosakan jika berlaku kejadian seperti petir, kilat dan sebagainya;	
r)	Semua pihak yang terlibat dalam pengurusan atau penggunaan peralatan ICT hendaklah bertanggungjawab dan mematuhi perkara berikut:	
	i. Memastikan semua peralatan ICT dikembalikan kepada Pegawai ICT Kementerian/Jabatan mengikut peraturan dan terma yang ditetapkan; dan	
	ii. Membatalkan atau menarik balik semua kebenaran, capaian ke atas peralatan ICT mengikut peraturan yang ditetapkan.	
7.2.2	**Media Storan**	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, *thumb drive, external drive* dan media storan lain. Media storan perlu dipastikan berada dalam keadaan yang baik dan selamat.		Pentadbir Sistem/Pegawai KPN

Bil.	Perkara	Tanggungjawab

Tindakan berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan ketersediaan maklumat yang disimpan adalah terjamin dan selamat:

a) Sediakan ruang penyimpanan yang kondusif, selamat dan sesuai dengan kandungan maklumat;

b) Mendapatkan kebenaran terlebih dahulu sebelum memasuki kawasan penyimpanan media storan. Kawasan ini adalah terhad kepada mereka yang dibenarkan sahaja;

c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;

d) Merekodkan pergerakan media storan yang dipinjam;

e) Mendapatkan kelulusan pemilik maklumat terlebih dahulu sebelum menghapuskan maklumat atau kandungan media storan;

f) Menghapuskan maklumat dan kandungan media storan dengan teratur dan selamat;

g) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;

h) Mewujudkan salinan pendua atau *backup* pada media storan yang lain bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;

i) Peralatan *backup* hendaklah diletakkan di tempat yang terkawal; dan

j) Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan.

Bil.	Perkara	Tanggungjawab
7.2.3	**Media Tandatangan Digital**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pegawai KPN hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	ICTSO/Pentadbir Sistem/Pegawai KPN
7.2.4	**Media Perisian dan Aplikasi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan KPN; b) Sistem maklumat dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c) Lesen perisian (*registration code*, *CD-keys* dan nombor siri) perlu disimpan berasingan daripada *CD-ROM*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	ICTSO/Pengurus ICT/Pentabir Sistem/Pegawai KPN

Bil.	Perkara	Tanggungjawab
7.2.5	**Penyelenggaraan Peralatan ICT**	
	Peralatan ICT hendaklah diselenggara dengan baik bagi menjamin kerahsiaan, integriti dan ketersediaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan ICT yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b) Memastikan peralatan ICT hanya boleh diselenggara oleh Pegawai KPN atau Pihak Ketiga yang dibenarkan sahaja; c) Bertanggungjawab memastikan setiap peralatan ICT diselenggara sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan; d) Menyemak dan menguji semua peralatan ICT sebelum dan selepas proses penyelenggaraan; dan f) Memaklumkan jadual penyelenggaraan yang telah ditetapkan atau berdasarkan keperluan kepada Pegawai KPN sebelum melaksanakan penyelenggaraan.	Pentabir Sistem/Pegawai KPN/Pihak Ketiga
7.2.6	**Pinjaman Peralatan ICT**	
	Peralatan ICT yang dipinjam adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mendapatkan kelulusan mengikut peraturan di bawah Pekeliling Perbendaharaan Tatacara Pengurusan Aset atau peraturan KPN bagi membawa keluar peralatan ICT tertakluk kepada tujuan yang dibenarkan; b) Pegawai KPN hendaklah memohon peminjaman peralatan ICT melalui sistem yang berkuatkuasa; c) Pegawai KPN perlu melindungi dan mengawal peralatan ICT sepanjang tempoh pinjaman;	Pentabir Sistem/Pegawai KPN/Pihak Ketiga

Bil.	Perkara	Tanggungjawab
	d) Memastikan aktiviti pinjaman dan pemulangan peralatan ICT direkodkan; dan e) Memastikan peralatan ICT yang dipulangkan dalam keadaan baik dan lengkap.	
7.2.7	**Peralatan ICT di Luar Premis KPN**	
	Bagi peralatan ICT yang dibawa keluar dari premis KPN, langkah-langkah keselamatan berikut hendaklah diambil: a) Peralatan ICT perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c) Memeriksa dan memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat Kerajaan. Maklumat perlu dihapuskan dari peralatan tersebut setelah disalin ke media storan yang lain.	Pegawai Aset/Pegawai KPN/Pihak ketiga
7.2.8	**Pelupusan Peralatan ICT**	
	Peralatan ICT yang hendak dilupuskan perlu melalui proses pelupusan mengikut Tatacara Pengurusan Aset Alih Kerajaan. Pelupusan peralatan ICT perlu dilakukan secara terkawal dan lengkap bagi memastikan tidak berlakunya kebocoran maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua data dan maklumat dalam peralatan ICT khususnya yang terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilaksanakan; dan b) Data dan maklumat dalam peralatan ICT yang akan dilupuskan hendaklah dihapuskan secara selamat.	Pegawai Aset/Pegawai KPN/Pihak Ketiga

Bil.	Perkara	Tanggungjawab
7.2.9	***Clear Desk dan Clear Screen***	
	Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif dan terperingkat terdedah sama ada di atas meja atau di paparan skrin apabila Pegawai KPN tidak berada di tempatnya. Langkah-langkah yang perlu diambil adalah dengan menggunakan kemudahan *screen saver with password*, *lock PC* atau log keluar apabila meninggalkan komputer.	Pegawai KPN
7.3	**Keselamatan Persekitaran**	
7.3.1	**Kawalan Persekitaran**	
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan peralatan ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa dan mengubahsuai hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah dipatuhi: a) Merancang dan menyediakan pelan keseluruhan susun atur kemudahan ICT, ruang atur pejabat dan sebagainya dengan teliti; b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c) Bahan mudah terbakar **DILARANG** disimpan di dalam kawasan penyimpanan peralatan ICT; d) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari peralatan ICT.	ICTSO/BKP

Bil.	Perkara	Tanggungjawab
	e) Pegawai KPN adalah **DILARANG** merokok atau menggunakan peralatan memasak seperti cerek elektrik, ketuhar gelombang mikro dan lain-lain berhampiran peralatan ICT; f) Peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dicapai dan dikendalikan; g) Semua peralatan perlindungan keselamatan hendaklah diperiksa sekurang-kurangnya dua (2) kali setahun dan diuji sekurang-kurangnya satu (1) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; h) Bilik sesalur telefon*/Building Main Distribution Frame* (BMDF) hendaklah sentiasa dikunci; dan i) Mematuhi peraturan yang telah ditetapkan oleh pihak berkuasa seperti Jabatan Bomba dan Penyelamat, Jabatan Kerja Raya dan sebagainya.	
7.3.2	**Bekalan Kuasa**	
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan hendaklah disalurkan mengikut voltan yang bersesuaian; b) Peralatan sokongan seperti *Uninterruptible Power Supply* (UPS) dan penjana elektrik (*electric generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data untuk mendapat bekalan kuasa berterusan; dan	ICTSO/Pegawai Keselamatan/ Pentadbir Pusat Data/Pentadbir Rangkaian/ Penyelenggara Bangunan

Bil.	Perkara	Tanggungjawab
	c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.	
7.3.3	**Kabel Peralatan ICT**	
	Kabel peralatan ICT hendaklah dilindungi kerana ia adalah salah satu komponen dalam sistem maklumat. Langkah-langkah keselamatan kabel adalah seperti berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel dengan menggunakan konduit untuk mengelakkan kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	ICTSO/Pentadbir Sistem/BKP
7.3.4	**Prosedur Kecemasan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap Pegawai KPN hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang telah ditetapkan; b) Setiap Pegawai KPN perlu melaporkan insiden kecemasan persekitaran kepada Pegawai Keselamatan; dan c) Pegawai Keselamatan perlu mengadakan, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa.	Pegawai Keselamatan/ Pegawai KPN

Bil.	Perkara	Tanggungjawab
7.4	**Keselamatan Dokumen Digital**	
7.4.1	**Dokumen Digital**	
	Bagi memastikan keselamatan maklumat, langkah-langkah pengurusan dokumen digital yang baik dan selamat seperti berikut hendaklah dipatuhi: a) Memastikan sistem dokumentasi atau penyimpanan dokumen digital adalah selamat; b) Kehilangan atau kerosakan semua jenis dokumen digital perlu dimaklumkan mengikut prosedur Arahan Keselamatan; c) Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen digital; d) Pergerakan dokumen digital terperingkat dan Rahsia Rasmi hendaklah mengikut prosedur keselamatan; e) Pelupusan dokumen digital hendaklah mengikut prosedur keselamatan yang sedang berkuatkuasa seperti Arahan Keselamatan dan tatacara Jabatan Arkib Negara; f) Dokumen digital terperingkat perlu dienkripsikan sebelum dihantar secara elektronik; dan g) Memastikan cetakan yang mengandungi maklumat terperingkat diambil segera dari pencetak.	ICTSO/ Pegawai KPN

BAB 8: KESELAMATAN OPERASI

Objektif : Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan baik dan selamat daripada sebarang ancaman dan gangguan.

Bil.	Perkara	Tanggungjawab
8.1	**Prosedur dan Tanggungjawab Operasi**	
8.1.1	**Pengendalian Prosedur Operasi**	
	Semua prosedur pengurusan operasi hendaklah dikenal pasti, didokumenkan, disimpan dan dihadkan capaian berdasarkan keperluan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur operasi hendaklah didokumenkan dengan jelas, teratur, dikemaskini dan sedia diguna pakai oleh Pegawai KPN; b) Setiap perubahan kepada prosedur operasi mestilah dikawal; c) Tugas dan tanggungjawab fungsi perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan peralatan ICT KPN; dan d) Kemudahan ICT untuk kerja-kerja pembangunan, pengujian dan operasi perlu diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.	ICTSO/Pentadbir Sistem/Pegawai KPN
8.1.2	**Pengurusan Perubahan**	
	Perubahan kepada organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang memberi kesan kepada keselamatan maklumat hendaklah dikawal. Pengurusan perubahan perlu mengambil kira tahap kritikal sistem dan proses yang terlibat. Perkara-perkara yang perlu	ICTSO/Pentadbir Sistem/Pegawai KPN

Bil.	Perkara	Tanggungjawab

dipatuhi adalah seperti berikut:

a) Mewujudkan prosedur pengurusan perubahan;

b) Merekodkan semua perubahan yang telah dipersetujui dan dilaksanakan;

c) Memantau pelaksanaan perubahan; dan

d) Menilai semula risiko perubahan.

8.1.3 Pengurusan Kapasiti

Kapasiti sistem ICT hendaklah dirancang, diurus dan dikawal dengan terperinci bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan operasi sistem ICT.

ICTSO/ Pentadbir Sistem

Keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

8.1.4 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian ataupun perubahan tidak sah ke atas persekitaran operasi. Perkara - perkara yang perlu dipatuhi:

ICTSO/Pentadbir Sistem

a) Mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan operasi;

b) Merekodkan semua penggunaan sumber yang dilaksanakan; dan

Bil.	Perkara	Tanggungjawab
	c) Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.	
8.2	**Pengurusan Penyampaian Perkhidmatan Pihak Ketiga**	
8.2.1	**Perkhidmatan Penyampaian Pihak Ketiga**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggara oleh pihak ketiga; dan b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh Pihak Ketiga perlu sentiasa dipantau, disemak semula dan diaudit secara berkala.	ICTSO/Pentadbir Sistem/Pihak Ketiga
8.3	**Perancangan dan Penerimaan Sistem**	
8.3.1	**Perancangan Kapasiti**	
	Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh Pentadbir Sistem bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO/ Pentadbir Sistem
8.3.2	**Penerimaan Sistem**	
	Semua sistem baharu (termasuklah sistem yang dikemaskini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Satu surat pengesahan penerimaan hendaklah dikeluarkan dengan persetujuan kedua-dua pihak.	Pengurus ICT/ Pentadbir Sistem

Bil.	Perkara	Tanggungjawab
8.4	**Perlindungan Daripada Perisian Berbahaya**	
	Memastikan peralatan ICT dilindungi daripada kod berbahaya seperti *virus*, *worm*, *trojan* dan lain-lain perisian untuk mengelakkan dari kerosakan.	
8.4.1	**Perlindungan Daripada *Malware***	
	Langkah-langkah pencegahan, pengesanan dan pemulihan untuk melindungi sistem ICT daripada gangguan adalah seperti berikut: a) Memasang sistem keselamatan seperti *antivirus, Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) untuk mengesan perisian atau program berbahaya mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah undang-undang bertulis yang berkuatkuasa; c) Mengimbas semua perisian atau sistem dengan *antivirus* sebelum menggunakannya; d) Mengemaskini perisian *antivirus* dengan *virus definition* yang terkini; e) Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan; f) Menyemak kandungan sistem maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; g) Melaksanakan dan menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; h) Memasukkan klausa tanggungan dalam sebarang	ICTSO/Pentadbir Sistem/Pegawai KPN

Bil.	Perkara	Tanggungjawab
	perjanjian yang ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;	
i)	Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan;	
j)	Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; dan	
k)	Melaksanakan Program Kesedaran Pengguna yang bersesuaian.	
8.5	***Backup***	
Memastikan salinan *backup* untuk maklumat dan perisian sistem disediakan dan diuji secara berkala selaras dengan polisi *backup* bagi tujuan kesinambungan operasi sistem maklumat.		
8.5.1	**Pelaksanaan *Backup***	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut:		ICTSO/Pentadbir Sistem
a)	Membuat salinan *backup* ke atas semua maklumat dan sistem perisian mengikut jadual yang ditetapkan atau apabila berlaku perubahan versi;	
b)	Menyimpan salinan *backup* di lokasi lain yang selamat; dan	
c)	Menguji sistem *backup* bagi memastikan ia dapat beroperasi dengan normal.	
8.6	**Pengurusan Media**	
Melindungi media daripada sebarang pendedahan, pengubahsuaian, pemindahan, pemusnahan dan gangguan perkhidmatan.		

Bil.	Perkara	Tanggungjawab
8.6.1	**Penghantaran dan Pemindahan Maklumat**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Melabelkan semua media mengikut tahap kerahsiaan sesuatu maklumat; b) Mengehadkan dan menentukan capaian media kepada Pegawai KPN yang dibenarkan sahaja; c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat; dan f) Media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut prosedur yang ditetapkan sekiranya tidak diperlukan.	Pentadbir Sistem/Pegawai KPN

BAB 9: KESELAMATAN KOMUNIKASI

Objektif : Melindungi keselamatan fasiliti pemprosesan maklumat dalam rangkaian.

Bil.	Perkara	Tanggungjawab
9.1	**Pengurusan Keselamatan Rangkaian**	
	Keselamatan rangkaian adalah elemen penting dalam memastikan komunikasi maklumat selamat dan terjamin.	
9.1.1	**Kawalan Infrastruktur Rangkaian**	
	Infrastruktur rangkaian hendaklah dirancang, diurus dan dikawal bagi melindungi keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah:	ICTSO/ Pentadbir Rangkaian
	a) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berkaitan dengan sistem rangkaian;	
	b) Peralatan keselamatan komunikasi seperti *firewall* hendaklah dipasang bagi memastikan hak capaian ke atas sistem dapat dilaksanakan seperti ditetapkan;	
	c) Sebarang cubaan menceroboh dan aktiviti yang boleh mengancam sistem maklumat KPN perlu dipantau dan dikesan melalui pemasangan peralatan keselamatan komunikasi seperti *Intrusion Prevention Sistem (IPS)*;	
	d) Peralatan rangkaian hendaklah diletakkan di lokasi yang bebas dari risiko seperti banjir, gegaran dan habuk;	
	e) Sebarang keperluan penyambungan rangkaian hendaklah melalui proses dan prosedur yang ditetapkan;	
	f) Penggunaan rangkaian tanpa wayar *(wireless) LAN* di KPN hendaklah mematuhi peraturan yang dikeluarkan	

Bil.	Perkara	Tanggungjawab
	oleh pihak berkenaan seperti MAMPU dan Majlis Keselamatan Negara (MKN); dan	
	g) Semua perisian berkaitan rangkaian dan keselamatan komunikasi seperti *sniffer* atau *network analyzer* adalah dilarang dipasang pada peralatan ICT kecuali mendapat kebenaran ICTSO.	
9.1.2	**Keselamatan Perkhidmatan Rangkaian**	
	Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat bagi menjamin kerahsiaan, integriti dan ketersediaan maklumat. Perkara-perkara yang perlu dipatuhi adalah:	Pentadbir Sistem/Pegawai KPN
	a) Mekanisma keselamatan komunikasi, tahap ketersediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara dalaman ataupun menggunakan sumber luar;	
	b) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan komunikasi di bawah kawalan KPN; dan	
	c) Sebarang aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam (PKPA) yang berkuat kuasa perlu disekat melalui penggunaan *Web Content Filtering.*	
9.1.3	**Pengasingan Rangkaian**	
	Pengasingan perkhidmatan rangkaian bertujuan untuk meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara–perkara yang perlu dipatuhi adalah:	Pentadbir Rangkaian

Bil.	Perkara	Tanggungjawab
	a) Mengenal pasti fungsi dan tanggungjawab Pegawai KPN; b) Had capaian Pegawai KPN ditentukan mengikut segmen rangkaian berdasarkan keperluan; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada Pegawai KPN yang dibenarkan sahaja; d) Mengemaskini had capaian Pegawai KPN dari semasa ke semasa mengikut keperluan; dan e) Segmen rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	
9.2	**Pemindahan Maklumat**	
	Memastikan keselamatan maklumat terjamin semasa pemindahan maklumat dengan entiti luar.	
9.2.1	**Prosedur Pemindahan Maklumat**	
	Prosedur ini bertujuan untuk mengendali, menyimpan, memindah, melindungi maklumat daripada didedah tanpa kebenaran atau salah guna dan memastikan keselamatan pemindahan maklumat dengan entiti luar terjamin. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengehadkan dan menentukan capaian kepada Pegawai KPN/Pihak Ketiga yang dibenarkan sahaja; b) Mengehadkan perkongsian data untuk tujuan rasmi dan yang dibenarkan sahaja; c) Polisi, prosedur dan kawalan pemindahan maklumat yang rasmi perlu diwujudkan untuk melindungi	ICTSO/Pentadbir Sistem/Pegawai KPN/Pihak Ketiga

Bil.	Perkara	Tanggungjawab
	pemindahan maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; d) Sebarang pemindahan maklumat di antara KPN dan Pihak Ketiga mestilah dikawal; dan e) Penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi Kerajaan perlu mendapat kelulusan Ketua Jabatan.	
9.2.2	**Perjanjian Pemindahan dan Kerahsiaan Maklumat**	
	a) *Non-Disclosure Agreement* (NDA) perlu diwujudkan bagi memastikan kerahsiaan, integriti dan ketersediaan (CIA) maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara KPN dengan Pihak Ketiga; dan b) Keperluan melindungi keselamatan maklumat yang merangkumi kerahsiaan, integriti dan ketersediaan hendaklah disemak secara berkala dan didokumenkan.	ICTSO/Pentadbir Sistem/Pegawai KPN/Pihak Ketiga
9.2.3	**Pengurusan E-mel**	
	Maklumat yang dihantar, diterima dan disimpan melalui e-mel KPN perlu dilindungi bagi mengelakkan capaian atau penyebaran maklumat yang tidak dibenarkan. Pegawai KPN layak menerima kemudahan perkhidmatan e-mel dengan kelulusan daripada Ketua Jabatan.	KSU/KP/ Pentadbir Sistem/Pegawai KPN

BAB 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif : Memastikan sistem maklumat yang dibangunkan secara dalaman ataupun luaran mempunyai ciri-ciri keselamatan yang kukuh daripada serangan siber.

Bil.	Perkara	Tanggungjawab
10.1	**Keperluan Keselamatan Sistem Maklumat**	
	Memastikan sistem maklumat yang dibangunkan secara dalaman/luaran perlulah mempunyai ciri-ciri keselamatan yang kukuh.	
10.1.1	**Analisis Keperluan dan Spesifikasi Keselamatan Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan; b) Semua sistem maklumat yang dibangunkan sama ada secara dalaman atau luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan berkaitan yang berkuat kuasa; dan c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem maklumat hendaklah mematuhi kawalan keselamatan.	ICTSO/Pentadbir Sistem/Pihak Ketiga
10.1.2	**Perlindungan Sistem Maklumat di Internet**	
	Sistem maklumat yang boleh dicapai melalui Internet perlu dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat dan pengubahsuaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah: a) Identiti Pegawai KPN/Pihak Ketiga yang diberi tahap capaian perlu dikenal pasti dan disahkan; b) Setiap Pegawai KPN/Pihak Ketiga perlu diberi peranan	Pengurus ICT/Pentadbir Sistem/Pentadbir Rangkaian/Pegawai KPN/Pihak Ketiga

Bil.	Perkara	Tanggungjawab
	mengikut skop dan tanggungjawab yang telah ditetapkan; dan	
	c) Memastikan Pihak Ketiga diberi penerangan mengenai keperluan mematuhi kontrak dan peraturan keselamatan yang ditetapkan dan menandatangani akuan pematuhan PKS.	
10.1.3	**Melindungi Transaksi Perkhidmatan Atas Talian**	
	a) Maklumat yang dihantar secara atas talian hendaklah dilindungi daripada penghantaran yang tidak lengkap, *misrouting*, pengubahsuaian dan pendedahan yang tidak dibenarkan; dan	ICTSO/Pentadbir Sistem/Pegawai KPN/Pihak Ketiga
	b) Sistem pengoperasian dan sistem maklumat hendaklah dilindungi daripada keterdedahan.	
10.1.4	**Validasi Data Input dan Output**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Sistem/ Pegawai KPN/Pihak Ketiga
	a) Data input bagi sistem maklumat perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan	
	b) Data output daripada sistem maklumat perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	
10.2	**Keselamatan Dalam Proses Pembangunan Dan Sokongan**	
	Memastikan *Secured Programming* dilaksanakan dalam kitar hayat pembangunan sistem maklumat.	
10.2.1	**Polisi Keselamatan Dalam Pembangunan Sistem Maklumat**	
	Tatacara pembangunan sistem maklumat yang mengambil kira aspek *Secured Programming* hendaklah diwujudkan dan	ICTSO/ Pengurus ICT

Bil.	Perkara	Tanggungjawab
	dilaksanakan dengan membangunkan Dokumen Pelan Pengurusan Keselamatan Maklumat (ISMP) semasa proses pembangunan sistem.	
10.2.2	**Prosedur Kawalan Perubahan Sistem Maklumat**	
	Prosedur kawalan perubahan hendaklah diwujudkan bagi mengawal sebarang perubahan sepanjang kitar hayat pembangunan sistem maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang ditetapkan dan pelaksanaan hanya mengikut keperluan sahaja; b) Perubahan atau pengubahsuaian ke atas perisian dan sistem maklumat hendaklah diuji, didokumenkan dan disahkan sebelum digunakan; dan c) Setiap perubahan kepada sistem pengoperasian perlu dikaji dan diuji untuk memastikan tiada sebarang masalah yang timbul.	ICTSO/Pengurus ICT/Pentadbir Sistem
10.2.3	**Semakan Teknikal Sistem Selepas Perubahan Platform**	
	Semakan dan pengujian terhadap sistem kritikal perlu dilaksanakan sekiranya berlaku perubahan terhadap sistem pengoperasian bagi memastikan fungsi dan operasi sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan sistem maklumat, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan; dan b) Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan.	ICTSO/Pengurus ICT/Pentadbir Sistem

Bil.	Perkara	Tanggungjawab
10.2.4	**Kawalan Terhadap Perubahan Kepada Perisian**	
	Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.	Pentadbir Sistem
10.2.5	**Prinsip Kejuruteraan Sistem Maklumat Yang Selamat**	
	Prinsip kejuruteraan sistem maklumat yang selamat hendaklah dibangunkan, didokumenkan, dikaji dan digunakan ke atas semua pelaksanaan sistem maklumat.	ICTSO/Pentadbir Sistem
10.2.6	**Persekitaran Pembangunan Sistem Maklumat Yang Selamat**	
	Persekitaran pembangunan sistem maklumat yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem maklumat.	Pentadbir Sistem
10.2.7	**Pembangunan Sistem Maklumat oleh Pihak Ketiga**	
	Sebarang aktiviti pembangunan sistem maklumat yang melibatkan Pihak Ketiga perlu dikawal selia dan dipantau. Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut: a) Memastikan spesifikasi perolehan mengandungi klausa tertentu berhubung keperluan keselamatan, sijil keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi pembangun sistem; b) Memastikan *Intellectual Property Right (*IPR) dan kod sumber menjadi hak milik kerajaan; c) Memasukkan klausa ke dalam kontrak yang membenarkan kerajaan melaksanakan semakan terhadap kod sumber; dan	Pengurus ICT/Pentadbir Sistem/Pihak Ketiga

Bil.	Perkara	Tanggungjawab
d)	Memasukkan klausa ke dalam kontrak yang membenarkan kerajaan mendapat hak pemilikan kod sumber dan melaksanakan penilaian semula risiko.	
10.2.8	**Ujian Keselamatan Sistem Maklumat**	
	Aktiviti pengujian penerimaan sistem hendaklah dilaksanakan ke atas sistem baru, naik taraf dan versi baru berdasarkan kriteria yang telah ditetapkan. Bagi memastikan integriti data, pengujian hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (*input*), peringkat pemprosesan data (*process*) dan peringkat penjanaan laporan (*output).*	Pengurus ICT/Pentadbir Sistem
10.2.9	**Ujian Penerimaan Sistem Maklumat**	
	Semua sistem maklumat baharu (termasuklah sistem maklumat yang dikemaskini/diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem/Pemilik Sistem
10.3	**Data Ujian**	
	Memastikan data yang digunakan untuk pengujian adalah terkawal.	
10.3.1	**Perlindungan Data Ujian**	
	Data ujian hendaklah bersesuaian, dilindungi dan dikawal.	Pentadbir Sistem/Pemilik Sistem

BAB 11: HUBUNGAN DENGAN PIHAK KETIGA

Objektif : Memastikan aset dilindungi sepenuhnya daripada akses yang tidak sewajarnya oleh Pihak Ketiga.

Bil	Perkara	Tanggungjawab
11.1	**Keselamatan Maklumat Dalam Hubungan Pihak Ketiga**	
11.1.1	**Polisi Keselamatan Maklumat Ke Atas Pihak Ketiga**	
	Pihak Ketiga adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa. Perkara–perkara yang perlu dipatuhi adalah seperti berikut: a) Pihak Ketiga hendaklah menandatangani Surat Akuan Pematuhan PKS KPN; b) Pihak Ketiga hendaklah menjalani ujian tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); dan c) Pihak Ketiga hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas.	Pengurus ICT/ Pihak Ketiga
11.1.2	**Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pihak Ketiga**	
	Perjanjian dengan Pihak Ketiga hendaklah merangkumi keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan perkhidmatan teknologi maklumat dan komunikasi.	Pengurus ICT/Pihak Ketiga
11.1.3	**Kawalan Keselamatan Maklumat Dengan Pembekal Utama Kepada Pihak Ketiga**	
	Perjanjian dengan Pihak Ketiga hendaklah meliputi risiko keselamatan yang merangkumi perkhidmatan ICT dan kesinambungan bekalan produk dengan pembekal utama kepada Pihak Ketiga.	ICTSO/Pengurus ICT/Pihak Ketiga

Bil	Perkara	Tanggungjawab
11.2	**Pengurusan Penyampaian Perkhidmatan Pihak Ketiga**	
	Untuk mengekalkan tahap keselamatan maklumat adalah sama seperti yang dipersetujui dalam perjanjian dengan Pihak Ketiga.	
11.2.1	**Pemantauan dan Penilaian Perkhidmatan Pihak Ketiga**	
	KPN hendaklah memantau, menyemak dan mengaudit perkhidmatan Pihak Ketiga secara berkala**.**	ICTSO/Pengurus ICT/Pemilik Projek
11.2.2	**Pengurusan Perubahan Perkhidmatan Pihak Ketiga**	
	Setiap perubahan perkhidmatan Pihak Ketiga hendaklah dilaksanakan secara teratur dan mengikut SOP yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Setiap perubahan mesti dimasukkan di dalam perjanjian bersama Pihak Ketiga; b) Perubahan yang dilakukan adalah untuk meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) Perubahan dalam perkhidmatan Pihak Ketiga hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran Pihak Ketiga dan subkontraktor.	ICTSO/Pengurus ICT/Pemilik Projek

BAB 12: PENGURUSAN INSIDEN KESELAMATAN SIBER

Objektif : Memastikan tindakan menangani insiden keselamatan siber diambil dengan cepat, tepat dan berkesan bagi memastikan perkhidmatan ICT KPN dapat beroperasi semula.

Bil.	Perkara	Tanggungjawab
12.1	**Pengurusan Insiden Dan Penambahbaikan Keselamatan Maklumat**	
	Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan siber supaya tidak menjejaskan imej KPN dan sistem penyampaian perkhidmatan.	
12.1.1	**Tanggungjawab Dan Prosedur**	
	Prosedur bagi mengurus insiden keselamatan siber perlu diwujudkan dan didokumenkan.	Pasukan CERT
12.1.2	**Pelaporan Insiden Keselamatan Siber**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua insiden keselamatan siber yang berlaku mesti dilaporkan kepada Pasukan CERT. Semua maklumat adalah SULIT dan tidak boleh didedahkan tanpa kebenaran daripada ICTSO; b) Mematuhi prosedur operasi standard (SOP) keselamatan siber KPN; c) Mengenal pasti semua jenis insiden keselamatan siber seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; d) Menyimpan jejak audit dan memelihara bahan bukti; dan e) Menyediakan dan melaksanakan pelan tindakan pemulihan.	Pasukan CERT/Pegawai KPN

Bil.	Perkara	Tanggungjawab
12.1.3	**Pelaporan Kelemahan Keselamatan Siber**	
	Insiden keselamatan siber adalah meliputi perkara-perkara berikut: **a) Pelanggaran Polisi (*Violation of Policy*)** Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar PKS. **b) Penghalangan Penyampaian Perkhidmatan (*Denial of Service*)** Ancaman ke atas keselamatan sistem maklumat komputer iaitu perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal termasuklah *Denial of Service* (DoS), *Distributed Denial of Service* (DDoS) dan sabotaj. **c) Pencerobohan (*Intrusion*)** Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem maklumat tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem maklumat, pindaan data dan pindaan kepada konfigurasi sistem maklumat. **d) Pemalsuan (*Forgery*)** Pemalsuan dan penyamaran identiti yang dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti dan maklumat serta penipuan.	Pasukan CERT/Pegawai KPN

Bil.	Perkara	Tanggungjawab
	e) ***Spam*** Spam adalah e-mel yang dihantar ke akaun orang lain oleh penghantar yang tidak dikenali dalam satu masa dan secara berulang kali. Ini menyebabkan kesesakan dan tindak balas rangkaian menjadi perlahan. **f)** ***Malicious Code*** Perisian atau kod pengaturcaraan yang dimasukkan ke dalam sistem maklumat tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware, adware* dan sebagainya. **g)** ***Harrassment/Threats*** Gangguan dan ancaman melalui e-mel, media sosial dan media elektronik yang bermotifkan personal/peribadi dan atas sebab tertentu. **h)** ***Attempts/Hack Threats/Information Gathering*** Percubaaan (samada gagal atau berjaya) untuk mencapai sistem maklumat atau data tanpa kebenaran. Termasuk sniffing, *spoofing, phishing, probing, war driving* dan *scanning.* **i)** **Kehilangan Fizikal (*Physical Loss*)** Kehilangan capaian disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.	
12.1.4	**Penilaian Dan Keputusan Insiden Keselamatan Siber**	
	KPN hendaklah mengklasifikasi dan menentukan keutamaan tindakan ke atas insiden keselamatan siber berasaskan keutamaan seperti berikut:	ICTSO/Pasukan CERT

Bil.	Perkara	Tanggungjawab
	Keutamaan 1: Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara. **Keutamaan 2:** i. Pencerobohan atau percubaan menceroboh melalui infrastruktur Internet ke atas peralatan rangkaian; ii. Penghalangan penyampaian perkhidmatan secara teragih (*Distributed Denial of Service*); iii. Serangan atau kelemahan terbaru (*New Vulnerabilities*); iv. Pencerobohan melalui pemalsuan identiti; v. Pengubahsuaian laman web, perisian, atau mana-mana komponen sistem maklumat tanpa pengetahuan, arahan atau persetujuan pihak yang berkenaan; dan vi. Gangguan sistem maklumat untuk pemprosesan data atau penyimpanan data tanpa kebenaran.	
12.1.5	**Pengumpulan Dan Pengendalian Bukti**	
	Maklumat mengenai insiden keselamatan siber perlu dikenalpasti, dikumpul, dianalisis dan disimpan bagi tujuan pengumpulan dan pengendalian bukti. Pasukan CERT hendaklah memastikan bahan bukti berkaitan insiden keselamatan siber dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan bukti seperti jejak audit, *backup* berkala dan *off-site backup* hendaklah mengikut tatacara pengendalian yang berkuat kuasa.	ICTSO/Pengurus ICT/Pasukan CERT

Bil.	Perkara	Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Melindungi integriti bahan bukti;

b) Mengumpul dan menyimpan bahan bukti bagi tujuan analisis;

c) Merekodkan semua maklumat insiden termasuk maklumat pegawai yang terlibat, perisian, perkakasan dan peralatan yang digunakan;

d) Memaklumkan kepada pihak berkuasa perundangan, seperti pegawai undang-undang dan polis (jika perlu);

e) Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang diperlukan (jika perlu); dan

f) Menyediakan laporan insiden kepada CIO.

BAB 13: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (PKP)

Objektif : Menjamin operasi perkhidmatan dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

Bil.	Perkara	Tanggungjawab
13.1	**Kesinambungan Perkhidmatan**	
	Ketua Jabatan bertanggungjawab memastikan perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	KSU/KP
13.2	**Pelan Kesinambungan Perkhidmatan (PKP) - Pelan Pemulihan Bencana**	
	Pelan Pemulihan Bencana hendaklah dibangunkan untuk menjamin kesinambungan perkhidmatan ICT supaya tiada gangguan dalam perkhidmatan KPN. Pelan ini perlulah mendapat perakuan oleh Ketua Jabatan dan meliputi perkara-perkara berikut: a) Melantik ahli Pasukan Pemulihan Bencana; b) Mengenal pasti dan mendokumenkan semua tanggungjawab dan prosedur kecemasan atau pemulihan; c) Melaksanakan prosedur-prosedur kecemasan dan simulasi pemulihan bencana bagi memastikan pemulihan dapat dilakukan dalam jangka masa yang telah ditetapkan seperti yang tertakluk dalam Pelan Pemulihan Bencana; d) Mengadakan program kesedaran dan latihan kepada pengguna mengenai prosedur kecemasan; e) Mengkaji dan mengemaskini pelan sekurang-kurangnya setahun sekali; f) Membuat *backup*; dan g) Mewujudkan Pusat Pemulihan Bencana di lokasi lain.	ICTSO/Pengurus ICT/Pasukan Pemulihan Bencana

Bil.	Perkara	Tanggungjawab
13.3	**Perubahan atau Pengecualian PKP**	
	Sekiranya terdapat perubahan/pengemaskinian atau pengecualian yang perlu dilakukan, permohonan secara bertulis termasuk keterangan dan kebenaran untuk pengecualian/ perubahan hendaklah dikemukakan kepada Ketua Jabatan.	KSU/KP/ Pegawai KPN
13.4	**Program Latihan dan Kesedaran Terhadap PKP**	
	Semua Pegawai KPN mesti mempunyai kesedaran dan mengetahui peranan masing-masing terhadap PKP. Ketua Jabatan bertanggungjawab dalam memastikan latihan dan program kesedaran terhadap PKP dilaksanakan setiap tahun.	KSU/KP/ Pegawai KPN
13.5	**Pengujian PKP**	
a)	PKP perlu diuji dua (2) tahun sekali atau selepas perubahan utama, atau yang mana terdahulu bagi memastikan semua pihak yang berkenaan mengetahui dan maklum akan pelaksanaannya;	KSU/KP/Pasukan Pemulihan Bencana/ Pegawai KPN
b)	Salinan PKP mestilah disimpan di lokasi berasingan bagi mengelakkan kerosakan akibat bencana di lokasi utama. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan;	
c)	Ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam Pasukan Pemulihan Bencana dan Pegawai KPN yang terlibat mengetahui tentang pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan;	
d)	Ketua Jabatan hendaklah memastikan salinan Pelan Kesinambungan Perkhidmatan sentiasa dikemas kini dan dilindungi seperti di lokasi utama; dan	

Bil.	Perkara	Tanggungjawab
e)	Komponen PKP seperti Pelan Pemulihan Bencana (*Disaster Recovery Plan* – DRP), Pelan Komunikasi Krisis (*Crisis Communication Plan* – CCP) dan Pelan Tindak Balas Kecemasan (*Emergency Response Plan* – ERP) perlu diuji dua (2) tahun sekali atau selepas perubahan utama, atau yang mana terdahulu.	
13.6	**Ketersediaan Kemudahan Pemprosesan Maklumat**	
	Semua sistem maklumat dan peralatan yang kritikal hendaklah mempunyai kemudahan *redundancy* dan diuji (*failover test*) keberkesanannya mengikut keperluan.	Pasukan Pemulihan Bencana

BAB 14: PEMATUHAN

Objektif : Untuk menghindari pelanggaran undang-undang jenayah dan sivil, perlembagaan, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

Bil.	Perkara	Tanggungjawab
14.1	**Pematuhan Polisi**	
	Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan bahawa pematuhan dan sebarang perlanggaran terhadap peraturan dielakkan. Langkah-langkah perlu bagi mengelakkan sebarang perlanggaran perundangan termasuklah memastikan setiap Pegawai KPN membaca, memahami dan mematuhi Polisi Keselamatan Siber dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.	KSU/KP
14.2	**Keperluan Perundangan**	
	Senarai perundangan dan peraturan yang berkuat kuasa dari semasa ke semasa perlu dipatuhi oleh semua Pegawai KPN adalah seperti di **LAMPIRAN B**.	Pegawai KPN
14.3	**Perlindungan dan Privasi Data Peribadi**	
	Semua Pegawai KPN perlu sedar bahawa data peribadi yang dijana dalam peralatan ICT bukan di bawah tanggungjawab KPN. KPN tidak menjamin kerahsiaan data peribadi yang disimpan dalam peralatan ICT. Untuk menjamin keselamatan dan untuk tujuan penyelenggaraan rangkaian, pegawai yang telah diberi kuasa perlu mengawasi peralatan ICT, sistem maklumat dan operasi rangkaian. KPN berhak mengaudit operasi rangkaian dan sistem maklumat secara berkala bagi memastikan ia mematuhi PKS. KPN perlu bertanggungjawab untuk memastikan semua maklumat peribadi digunakan mengikut peraturan bagi	Pegawai KPN

Bil.	Perkara	Tanggungjawab
	mengelakkan penyalahgunaan maklumat. Pendedahan maklumat peribadi tentang Pegawai KPN kepada Pihak Ketiga hendaklah dielakkan kecuali: a) Dikehendaki oleh undang-undang atau peraturan; b) Dengan persetujuan yang jelas dan nyata daripada Pegawai KPN tersebut; atau c) Setelah menerima persetujuan bertulis daripada Pihak Ketiga di mana maklumat akan dilindungi dengan tahap keselamatan dan privasi yang mencukupi seperti yang ditentukan oleh Pejabat Undang-undang serta perjanjian jelas diperoleh daripada pengurusan sumber manusia; dan d) Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pengeluaran yang tidak sah mengikut undang-undang, peraturan, kontrak dan keperluan KPN.	
14.4	**Semakan Keselamatan Siber**	
	Semakan keselamatan siber mestilah diambil kira seperti berikut: a) Pematuhan pemeriksaan ke atas Polisi Keselamatan Siber, piawaian dan prosedur perlu dilakukan secara tahunan. Pemeriksaan ini mestilah melibatkan usaha bagi menentukan kawalan yang mencukupi dan dipatuhi; b) Pengauditan perlu dilaksanakan sekurang-kurangnya sekali setahun terhadap infrastruktur sistem maklumat bagi meminimakan ancaman dan meningkatkan ketersediaan sistem; dan c) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem pengoperasian perlu dirancang dan dipersetujui	ICTSO/Pengurus ICT

Bil.	Perkara	Tanggungjawab
	bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	
14.5	**Pelanggaran Perundangan**	
	KPN mesti mengambil tindakan tatatertib dan undang-undang ke atas Pegawai KPN atau Pihak Ketiga yang terlibat dalam semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan yang membahayakan maklumat terperingkat di bawah Akta Rahsia Rasmi 1972.	KSU/KP/UI/PUU
14.6	**Akuan Pematuhan Polisi Keselamatan Siber**	
	Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan semua Pegawai KPN dan Pihak Ketiga menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber seperti di **LAMPIRAN A1** dan **LAMPIRAN A2 .**	KSU/KP/Pegawai KPN/Pihak Ketiga
14.7	**Pematuhan Terhadap Hak Harta Intelek (*Intellectual Property Rights*)**	
	Prosedur pengawalan hendaklah dilaksanakan bagi memastikan pematuhan kepada perundangan, peraturan dan keperluan kontrak berkaitan produk yang mempunyai IPR termasuk perisian *proprietary*.	ICTSO

LAMPIRAN A1

AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN PERPADUAN NEGARA (KPN)

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber KPN; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan tatatertib yang sewajarnya dan tindakan undang-undang yang berkaitan boleh dikenakan ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT,

.....

(Tandatangan & Cop Jawatan)

Kementerian Perpaduan Negara

Tarikh : .....

* Polisi Keselamatan Siber KPN boleh dicapai menerusi www.perpaduan.gov.my

LAMPIRAN A2

AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN PERPADUAN NEGARA (KPN)

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Syarikat : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami, dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber KPN;
2. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub dalam Polisi Keselamatan Siber KPN; dan
3. Sekiranya saya atau mana-mana individu yang mewakili syarikat ini didapati melanggar dasar yang telah ditetapkan, maka saya sebagai wakil syarikat bersetuju tindakan undang-undang boleh diambil ke atas sesiapa yang terlibat mengikut peruntukan-peruntukan undang-undang sedia ada yang sedang berkuatkuasa.

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT,

.....

(Tandatangan & Cop Jawatan)

Kementerian Perpaduan Negara

Tarikh : .....

* Polisi Keselamatan Siber KPN boleh dicapai menerusi www.perpaduan.gov.my

LAMPIRAN B

RUJUKAN

SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan (Semakan dan Pindaan 2015);
2. Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
4. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisma Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
6. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
7. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
8. Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
9. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
10. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
11. Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan;
12. Akta Tandatangan Digital 1997;
13. Akta Rahsia Rasmi 1972;
14. Akta Jenayah Komputer 1997;
15. Akta Hak Cipta (Pindaan) Tahun 1997;
16. Akta Komunikasi dan Multimedia 1998;

17. Perintah - Perintah Am;
18. Arahan Perbendaharaan;
19. Arahan Teknologi Maklumat 2007;
20. Garis Panduan Keselamatan MAMPU 2004;
21. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
22. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan;
23. Arahan Teknologi Maklumat dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007);
24. Pekeliling Am Bil. 1 Tahun 2009 – Manual Pengurusan Aset Menyeluruh Kerajaan;
25. Surat Pekeliling Am Bilangan 1 Tahun 2009 Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan;
26. Surat Arahan Ketua Setiausaha Negara – Langkah - Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain - Lain Peralatan Komunikasi ICT Tanpa Kebenaran (Tarikh : 31 Januari 2007);
27. Surat Arahan Ketua Pengarah MAMPU – Amalan Terbaik Penggunaan Media Jaringan Sosial (Tarikh : 8 April 2011);
28. Surat Arahan Ketua Pengarah MAMPU – Pemantapan Penggunaan Dan Pengurusan E-Mel. (Tarikh : 1 Julai 2010);
29. Surat Arahan Ketua Pengarah MAMPU – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam. (5 Mac 2010);
30. Surat Arahan Ketua Pengarah MAMPU – Garis Panduan Transisi Protokol Internet Versi 6 (IPV6) Sektor Awam. (Tarikh : 4 Januari 2010);
31. Surat Arahan Ketua Pengarah MAMPU – Penggunaan Media Jaringan Sosial Di Sektor Awam. (Tarikh : 19 November 2009);
32. Surat Arahan Ketua Pengarah MAMPU – Penggunaan Smartphone, Personel Digital Assistant Dan Alat Komunikasi Mudah Alih Sebagai Saluran Komunikasi Tambahan (Tarikh : 15 September 2009);
33. Surat Arahan Ketua Pengarah MAMPU – Pengaktifan Fail Log Server (Tarikh : 23 Mac 2009);

34. Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam (Ogos 2010);
35. Arahan Teknologi Maklumat Dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007);
36. Garis Panduan IT Outsourcing (Oktober 2006);
37. Garis Panduan Penyimpanan dan Pemeliharaan Rekod Elektronik Sektor Awam;
38. Arahan 20 (Semakan Semula) – Dasar dan Mekanisma Pengurusan Bencana Negara;
39. Arahan 24 - Dasar Dan Mekanisma Pengurusan Krisis Siber Negara;
40. Pekeliling Am Bil. 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam;
41. Rancangan Malaysia ke-11;
42. Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam;
43. Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam 25 Januari 2015;
44. Dasar Kriptografi Negara 12 Julai 2013;
45. Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology* ICT Kerajaan SPP 3/2013;
46. Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan;
47. Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013;
48. Arahan Ketua Pegawai Keselamatan Kerajaan 5 jun 2012 – Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam;
49. PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua);
50. Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 Nov 2010;
51. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam, 22 Jan 2010;
52. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan, 23 Nov 2007;

53. Arahan Ketua Setiausaha Negara Bil. 1 Tahun 2007 – Langkah-Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-Lain Peralatan Komunikasi ICT Tanpa Kebenaran Atau Kuasa Yang Sah Di Agensi-Agensi Kerajaan;
54. Akta 709 – Akta Perlindungan Data Peribadi 2010;
55. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) Di Agensi-Agensi Kerajaan, 20 Oktober 2006;
56. Akta 658 – Akta Perdagangan Elektronik 2006;
57. Akta 629 – Akta Arkib Negara 2003;
58. Akta 606 – Akta Cakera Optik 2000;
59. Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987);
60. Akta 298 – Kawasan Larangan Tempat Larangan 1959;
61. Akta 56 – Akta Keterangan 1950;
62. National Cyber Security Policy (NCSP);
63. Guideline to Determine Information Security Professionals Requirement for the CNII Agencies /Organisations;
64. Arahan Tetap Sasaran Penting;
65. Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara;
66. Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi;
67. Perintah Am Bab D; dan
68. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA) versi 1.0 April 2016.