



POLISI KESELAMATAN SIBER JABATAN WILAYAH PERSEKUTUAN VERSI 2023



Jabatan Wilayah Persekutuan
Jabatan Perdana Menteri
Blok 1 & Blok 2, Menara Seri Wilayah
Presint 2, 62100 Putrajaya

11 April 2023

ISI KANDUNGAN

BAB	KANDUNGAN	MUKA SURAT
	Pengenalan	1
	Objektif	1
	Pernyataan Polisi	1
	Skop	2
	Prinsip-prinsip	4
	Singkatan dan Takrifan	7
BAB 1:	Pelaksanaan Polisi	8
BAB 2:	Organisasi Keselamatan Siber	9
BAB 3:	Keselamatan Sumber Manusia	16
BAB 4:	Pengurusan Aset	19
BAB 5:	Pengurusan Kawalan Capaian	26
BAB 6:	Kriptografi	32
BAB 7:	Keselamatan Fizikal dan Persekitaran	33
BAB 8:	Keselamatan Operasi	45
BAB 9:	Keselamatan Komunikasi	51
BAB 10:	Perolehan, Pembangunan dan Penyelenggaraan Sistem	55
BAB 11:	Hubungan dengan Pembekal	60
BAB 12:	Pengurusan Insiden Keselamatan Siber	62
BAB 13:	Pengurusan Kesyinambungan Perkhidmatan (PKP) (<i>BUSINESS CONTINUITY MANAGEMENT (BCM)</i>)	67
BAB 14:	Pematuhan	70
	Rujukan	
	Lampiran	

PENGENALAN

Polisi Keselamatan Siber (PKS) Jabatan Wilayah Persekutuan (JWP) mengandungi peraturan-peraturan yang mesti dibaca, difahami dan dipatuhi semasa menggunakan aset Teknologi Maklumat dan Komunikasi atau *Information and Communication Technology* (ICT) JWP. Polisi ini juga menerangkan tanggungjawab dan peranan pengguna ICT JWP dalam melindungi aset ICT JWP.

OBJEKTIF

PKS JWP diwujudkan untuk menjamin kesinambungan urusan jabatan dengan meminimumkan kesan insiden keselamatan siber.

Objektif utama PKS JWP adalah seperti berikut:

- a) Memastikan kelancaran operasi JWP yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT JWP;
- b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat akibat kesan kegagalan atau kelemahan aspek kerahsiaan, integriti, tidak boleh disangkal, ketersediaan dan kesahihan;
- c) Mencegah salah guna atau kecurian aset ICT Jabatan;
- d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan aset ICT; dan
- e) meningkatkan tahap kesedaran keselamatan siber kepada para kakitangan, pengguna dan pihak luaran.

PERNYATAAN POLISI JWP

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

Keselamatan siber adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan. Terdapat empat (4) komponen asas keselamatan maklumat iaitu:

- a) Melindungi maklumat rasmi JWP dari capaian tanpa kuasa yang sah;

- b) Menjamin setiap maklumat adalah tepat, lengkap dan terkini;
- c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
- d) Memastikan akses hanya diberikan kepada pengguna yang sah dan penerimaan maklumat daripada sumber yang sah.

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

- a) **KERAHSIAAN** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
- b) **INTEGRITI** - Data dan maklumat hendaklah tepat, lengkap dan terkini. Ia hanya boleh diubah dengan cara yang dibenarkan;
- c) **TIDAK BOLEH DISANGKAL** - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
- d) **KESAHIHAN** - Data dan maklumat hendaklah dijamin kesahihannya; dan
- e) **KETERSEDIAAN** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, analisa tahap risiko aset ICT dikenalpasti, seterusnya mengambil tindakan untuk merancang dan mengawal risiko berkenaan.

SKOP

Aset ICT JWP merangkumi maklumat, platform aplikasi dan perisian, peranti fizikal dan sistem, aliran data, manusia, sistem luaran serta sumber luaran. PKS JWP menetapkan keperluan-keperluan asas seperti berikut:

- a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu 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 untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, PKS JWP ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat

salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

Skop PKS jabatan meliputi perkara berikut:

- a) **Maklumat** : Pangkalan data dan fail data, kontrak dan perjanjian, dokumentasi sistem, maklumat penyelidikan, manual pengguna, bahan latihan, prosedur operasi dan sokongan, pelan kesinambungan perkhidmatan, *fallback arrangements*, jejak audit (*audit trails*) dan maklumat arkib;
- b) **Platform Aplikasi dan Perisian** : Perisian aplikasi, perisian sistem, perisian pembangunan (*development tools*) dan utiliti (*utilities*);
- c) **Peranti Fizikal dan Sistem** : Peralatan komputer, peralatan komunikasi, media mudah alih dan lain-lain peralatan;
- d) **Aliran Data** : Merujuk kepada aliran transaksi data menggunakan saluran komunikasi yang dikenal pasti, direkodkan dan dikaji semula secara berkala seperti e-mel rasmi dan ruang storan pengkomputeran awan;
- e) **Sistem Luaran** : Sistem bukan milik JWP yang dihubungkan dengan sistem JWP;
- f) **Sumber Luaran** : Perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi JWP seperti perkhidmatan pengkomputeran awan dan komunikasi, utiliti umum seperti pencahayaan, elektrik dan pendingin hawa;

Contoh perkhidmatan sumber luaran ialah:

- i) Perisian Sebagai Satu Perkhidmatan
 - ii) Platform Sebagai Satu Perkhidmatan
 - iii) Infrastruktur Sebagai Satu Perkhidmatan
 - iv) Storan Pengkomputeran Awan
 - v) Pemantauan Keselamatan
- g) **Manusia** : Kelayakan, kemahiran dan pengalaman; dan
 - h) **Aset tidak nyata (*intangibles*)** : Seperti reputasi dan imej organisasi.

Semua warga jabatan adalah bertanggungjawab memastikan dan memelihara maklumat dan data berdasarkan perkara berikut:

- a) 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.

- b) Semua maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta melindungi kepentingan jabatan, perkhidmatan dan masyarakat.
- c) Mengenalpasti semua maklumat yang dijana atau dikumpul dan diasingkan mengikut kategori maklumat seperti Maklumat Rahsia Rasmi, Maklumat Rasmi, Maklumat Pengenalan Diri dan Data Terbuka.
- d) Bagi memastikan keselamatan maklumat yang berterusan, PKS merangkumi perlindungan semua bentuk maklumat dan data kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan, dalam penghantaran dan yang dibuat salinan keselamatan. Ini dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan/prosedur dalam pengendalian maklumat dan aset.

PRINSIP-PRINSIP

Prinsip PKS ini adalah seperti berikut:

- a) **Prinsip Perlu Tahu**
Capaian dibenarkan dan dihadkan kepada pengguna tertentu atas dasar “perlu tahu” berdasarkan klasifikasi maklumat dan tahap tapisan keselamatan pengguna.
- b) **Hak Keistimewaan Minimum**
Hak capaian kepada pengguna dimulai pada tahap yang paling minimum. Kelulusan adalah perlu bagi membolehkan capaian pada tahap yang lebih tinggi.
- c) **Kawalan Capaian Berdasarkan Peranan**
Capaian sistem dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.
- d) **Peminimuman Data**
Menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.
- e) **Akauntabiliti**
Setiap pengguna adalah bertanggungjawab ke atas semua tindakan terhadap kemudahan ICT jabatan yang disediakan. Tanggungjawab pengguna termasuk perkara berikut:

- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
 - ii. Memeriksa maklumat dan menentukan ianya sentiasa tepat dan lengkap;
 - iii. Menentukan maklumat sedia untuk digunakan;
 - iv. Menjaga kerahsiaan maklumat; dan
 - v. Mematuhi langkah dan garis panduan keselamatan siber yang ditetapkan.
- f) Pengasingan Tugas
- Setiap tugas, proses dan persekitaran pelaksanaan ICT hendaklah dipisahkan dan diasingkan sebaik mungkin untuk mengekalkan integriti dan perlindungan keselamatan daripada kesilapan dan penyalahgunaan. Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:
- i. Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;
 - ii. Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji; dan
 - iii. Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.
- g) Pengauditan
- Pengauditan adalah tindakan untuk mengenal pasti insiden atau keadaan yang mengancam keselamatan. Pengauditan adalah penting dalam menjamin akauntabiliti seperti berikut:
- i. Mengesan pematuhan atau pelanggaran polisi keselamatan siber;
 - ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran polisi keselamatan siber; dan
 - iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran polisi keselamatan siber.
- h) Pematuhan
- Prinsip ini penting untuk mengelakkan pelanggaran polisi melalui tindakan berikut:
- i. Mewujudkan proses yang sistematik khususnya dalam menjamin keselamatan siber untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan siber yang telah dikuatkuasakan;
 - ii. Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan siber yang dikenal pasti;

- iii. Melaksanakan program pemantauan keselamatan siber secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan siber dipatuhi; dan
 - iv. Menkuatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan siber dan seterusnya mengambil tindakan pembedahan.
- i) Pemulihan
- Pemulihan adalah untuk memastikan ketersediaan dan kebolehcapaian dengan meminimumkan gangguan atau kerugian akibat daripadanya adalah seperti berikut:
- i. Merancang dan menguji Pelan Pemulihan Bencana (DRP); dan
 - ii. Melaksanakan amalan terbaik dalam pelaksanaan ICT.
- j) Saling Bergantung
- Prinsip keselamatan siber adalah saling lengkap-melengkapi dan hendaklah dipatuhi bagi jaminan keselamatan siber yang berkesan. Tindakan mempelbagaikan pendekatan dalam menyusun strategi mekanisme keselamatan siber mampu meningkatkan tahap keselamatan siber.

SINGKATAN DAN TAKRIFAN

BCM	<i>Business Continuity Management</i>
BCP	<i>Business Continuity Plan</i>
BPM	Bahagian Pengurusan Maklumat
BKP	Bahagian Khidmat Pengurusan
CCP	<i>Crisis Communication Plan / Pelan Komunikasi Krisis</i>
CSIRT	<i>Computer Security Incident Response Team</i>
CIO	<i>Chief Information Officer</i>
CGSO	<i>Chief Government Security Officer / Ketua Pegawai Keselamatan Kerajaan</i>
CNII	<i>Critical National Information Infrastructure / Infrastruktur Maklumat Kritikal Negara</i>
DDOS	<i>Distributed Denial of Service</i>
DRP	<i>Disaster Recovery Plan / Pelan Pemulihan Bencana</i>
ERP	<i>Emergency Response Plan / Pelan Tindak Balas Kecemasan</i>
National CERT	<i>National Computer Emergency Response Team</i>
ICT	<i>Information and Communication Technology</i>
ICTSO	<i>Information and Communication Technology Security Officer</i>
ID	<i>Identity</i>
IDS	<i>Intrusion Detection System</i>
IPS	<i>Intrusion Prevention System</i>
ISMP	<i>Information System Management Planning / Pelan Pengurusan Keselamatan Maklumat</i>
ISMS	<i>Information Security Management System / Sistem Pengurusan Keselamatan Maklumat</i>
JPICT	Jawatankuasa Pemandu ICT
KP	Ketua Pengarah
PB	Pengarah Bahagian
LAN	<i>Local Area Network</i>
MAMPU	<i>Malaysia Administrative Modernisation and Management Planning Unit / Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia</i>
JWP	Jabatan Wilayah Persekutuan
PKI	<i>Public Key Infrastructure</i>
UPS	<i>Uninterruptable Power Supply</i>

BAB 1: POLISI KESELAMATAN SIBER

Objektif: Memastikan hala tuju pengurusan perlindungan maklumat adalah selaras dengan keperluan perkhidmatan jabatan dan peraturan serta undang-undang.

Bil.	Perkara
1.1 Pelaksanaan Polisi Keselamatan Siber JWP	
	PKS ini dilaksanakan oleh KP dengan dibantu oleh Jawatankuasa Pemandu ICT yang terdiri daripada CIO, ICTSO dan lain-lain pegawai yang dilantik.
1.2 Penyebaran Dasar	
	Dasar ini perlu disebar kepada semua pengguna.
1.3 Pemakaian Polisi	
	PKS ini terpakai kepada semua kakitangan jabatan dan juga pihak ketiga yang berurusan dengan jabatan.
1.4 Penyelenggaraan Polisi	
	<p>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 siber adalah dianggap perubahan utama dan hendaklah mendapat pengesahan JPICT Jabatan.</p> <p>Prosedur semakan semula polisi ini adalah seperti berikut:</p> <ol style="list-style-type: none"> a) Menyemak sekurang-kurangnya satu (1) kali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan atau perubahan secara bertulis kepada Pengurusan JWP; dan c) Memaklumkan pindaan atau perubahan polisi yang telah dipersetujui kepada semua pengguna.

BAB 2: ORGANISASI KESELAMATAN SIBER

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

Bil.	Perkara
2.1 Organisasi Keselamatan Siber	
2.1.1	Peranan dan tanggungjawab KP
	<p>Peranan dan tanggungjawab KP adalah seperti berikut:</p> <ol style="list-style-type: none"> a) Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber jabatan.; b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategi keselamatan siber jabatan; c) Merancang, menyelaraskan dan menyeragamkan pelaksanaan program/projek-projek keselamatan siber jabatan supaya selaras dengan Pelan Strategik Pendigitalan Jabatan; d) Memastikan keperluan sumber bagi keselamatan siber jabatan adalah mencukupi; dan e) Memastikan pelaksanaan penilaian risiko keselamatan siber jabatan.
2.1.2	Peranan dan tanggungjawab Ketua Pegawai Maklumat (CIO)
	<p>KP bertanggungjawab melantik CIO di jabatan. Peranan dan tanggungjawab CIO adalah seperti berikut:</p> <ol style="list-style-type: none"> a) Membantu KP dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber; b) Menentukan keperluan dan bertanggungjawab ke atas perkara-perkara berkaitan dengan keselamatan siber jabatan; dan c) Membangun dan menyelaraskan pelaksanaan program kesedaran dan latihan keselamatan siber.
2.1.3	Peranan dan tanggungjawab Pengurus ICT
	<p>Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:</p> <ol style="list-style-type: none"> a) Memastikan kajian semula dan pelaksanaan kawalan keselamatan siber selaras dengan keperluan jabatan; b) Memastikan ancaman atau insiden keselamatan siber dilaporkan kepada CIO;

Bil.	Perkara
	<ul style="list-style-type: none"> c) Menentukan kawalan capaian pengguna terhadap aset ICT; dan d) Memastikan penyimpanan rekod, bahan bukti dan laporan ancaman atau insiden keselamatan siber jabatan dilaksanakan dengan berkesan.
2.1.4	Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO)
	<p>Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:</p> <ul style="list-style-type: none"> a) Merancang, melaksana, mengurus dan memantau program keselamatan siber jabatan; b) Menguatkuasakan penggunaan PKS; c) Memberikan penerangan dan pendedahan berkenaan PKS jabatan kepada pengguna; d) Mewujudkan garis panduan dan prosedur selaras dengan keperluan PKS; e) Melaksanakan pengurusan risiko keselamatan siber; f) Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) Memberikan amaran kepada agensi terhadap kemungkinan berlakunya ancaman keselamatan siber seperti virus komputer dan penggodam serta memberi khidmat nasihat dan bantuan teknikal bagi menyediakan langkah perlindungan yang bersesuaian; h) Melaporkan insiden keselamatan siber kepada pengurusan jabatan; 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.
2.1.5	Peranan dan Tanggungjawab Pentadbir Sistem ICT
	<p>Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:</p> <ul style="list-style-type: none"> a) Menjaga kerahsiaan maklumat keselamatan siber; b) Mengambil tindakan segera apabila dimaklumkan mengenai sebarang perubahan pengguna dalaman/ luaran/ asing berkaitan pengurusan ICT; c) Menentukan pelaksanaan tahap capaian kemudahan ICT adalah bertepatan dengan arahan pemilik maklumat;

Bil.	Perkara
	<ul style="list-style-type: none"> d) Memantau dan menyediakan laporan aktiviti penggunaan dan capaian pengguna; e) Mengenal pasti dan melaporkan aktiviti tidak normal berkaitan ICT kepada pengurus ICT; dan f) Menyimpan dan menganalisis rekod jejak audit.
2.1.6	Peranan dan Tanggungjawab Pengguna
	<p>Pengguna mempunyai peranan dan tanggungjawab seperti berikut:</p> <ul style="list-style-type: none"> a) Membaca, memahami dan mematuhi PKS jabatan; b) Menjaga kerahsiaan maklumat berkaitan penggunaan ICT; c) Mengikuti dan menghayati program kesedaran keselamatan siber; d) Menandatangani Akuan Pematuhan PKS seperti di LAMPIRAN B atau yang setara dengannya; dan e) Melaporkan aktiviti yang tidak normal berkaitan ICT kepada BPM.
2.2 Jawatankuasa Pemandu ICT (JPICT) JWP	
	<p>Bidang Tugas Jawatankuasa Pemandu ICT JWP</p> <ul style="list-style-type: none"> a) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT JWP; b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT JWP dan semua agensi di bawah; c) Merancang dan menyelaras pembangunan program/projek ICT JWP dan semua agensi di bawah supaya selaras dengan pelan strategik JWP dan pelan strategik pendigitalan; d) Menyelaraskan dan menyeragamkan pembangunan dan pelaksanaan ICT antara JWP dan semua agensi di bawah dengan pelan strategik organisasi dan pelan strategik pendigitalan Sektor Awam; e) Mempromosi dan menggalakkan perkongsian pintar projek ICT antara Jabatan dan semua agensi di bawah; f) Merancang dan menentukan langkah-langkah keselamatan siber; g) Mengikuti dan memantau perkembangan program ICT JWP dan semua agensi di bawah, serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pembangunan dan pelaksanaan ICT;

Bil.	Perkara
	<ul style="list-style-type: none"> h) Menilai dan meluluskan semua perolehan ICT JWP dan semua agensi di bawah berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan; i) Menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi JWP dan semua agensi di bawah kepada Jawatankuasa Teknikal ICT Sektor Awam (JTISA) untuk kelulusan teknikal; j) Mengemukakan laporan projek ICT yang diluluskan diperingkat JPICT JWP dan dibuat perolehan kepada JTISA; dan k) Mengemukakan laporan kemajuan projek ICT bagi JWP dan semua agensi di bawah yang telah diluluskan oleh JTISA kepada JTISA mengikut tempoh yang telah ditetapkan.
2.3 Jawatankuasa ISMS JWP	
	<p>Peranan dan tanggungjawab Jawatankuasa ISMS JWP adalah seperti berikut:</p> <ul style="list-style-type: none"> a) Memantau pelaksanaan pensijilan ISMS ke atas skop yang telah dikenal pasti; b) Menyemak skop, pernyataan dasar ISMS dan <i>Statement of Applicability</i> (SOA); c) Menetapkan kriteria penerimaan risiko, tahap risiko dan <i>risk treatment plan</i>; d) Memantau dan menyemak penemuan awal penilaian risiko; e) Menyediakan cadangan struktur organisasi ISMS; f) Memantau dan menyemak keputusan dan tindakan Mesyuarat Kajian Semula ISMS; g) Memantau, menyemak dan memperakui dokumen dan rekod pelaksanaan ISMS; h) Memohon pensijilan ISMS; dan i) Memantau pelaksanaan tindakan pembetulan/penambakan dan pencegahan.
2.4 Tanggungjawab CSIRT JWP	
	<p>2.4.1 Tanggungjawab CSIRT JWP meliputi semua bidang tugas pengurusan dan pengendalian insiden keselamatan siber termasuklah agensi di bawah seliaannya seperti yang berikut:</p> <ul style="list-style-type: none"> a) Memantau, mengesan insiden, menerima, dan mengesahkan aduan

Bil.	Perkara
	<p>insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber.</p> <p>b) Merekod dan menjalankan siasatan awal terhadap insiden yang diterima.</p> <p>c) Melaksanakan pengurusan dan pengendalian insiden keselamatan siber serta mengambil tindakan awal pemulihan.</p> <p>d) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan.</p> <p>e) Melaporkan insiden keselamatan siber kepada <i>National Cyber Coordination and Command Centre (NC4)</i>.</p> <p>f) Menasihati agensi di bawah seliaannya mengambil tindakan pemulihan dan pengukuhan.</p> <p>g) Menyebarkan makluman/amaran berkaitan insiden kepada agensi lain di bawah seliaannya.</p> <p>h) Memastikan faillog disimpan sekurang-kurangnya enam bulan di tempat yang selamat.</p> <p>i) Apabila berlakunya insiden keselamatan siber, pengarah CSIRT JWP hendaklah menggerakkan ahli CSIRT JWP untuk mengambil tindakan seperti yang berikut:</p> <ul style="list-style-type: none"> i) Mengurus dan mengambil tindakan terhadap insiden yang berlaku sehingga keadaan pulih. ii) Mengaktifkan BCP dan/atau DRP jika perlu. iii) Melapor dan memaklumkan insiden keselamatan siber kepada NC4. iv) Menentukan sama ada insiden ini perlu dilaporkan kepada agensi

Bil.	Perkara
	penguatkuasaan undang-undang.
2.5 Juruaudit	
	<ul style="list-style-type: none"> a) Mengkaji dan menilai kawalan ke atas pematuhan dan pemantauan keselamatan siber berdasarkan dasar, <i>standard</i> dan prosedur keselamatan maklumat; dan b) Menilai kawalan pengurusan keselamatan aset ICT.
2.6 Penasihat Undang-Undang	
	<ul style="list-style-type: none"> a) Menyediakan khidmat nasihat perundangan bagi memastikan aktiviti ICT Jabatan dapat dijalankan sepenuhnya berdasarkan undang-undang dan peraturan yang berkuat kuasa; b) Menyemak kontrak bagi memastikan terma dan syarat kontrak memelihara kepentingan Kerajaan dan selaras dengan peruntukan perundangan yang sedang berkuat kuasa; c) Memberi khidmat nasihat perundangan dalam hal yang berkaitan dengan obligasi serta tanggungan pihak Kerajaan dalam mana-mana kontrak (sekiranya ada); dan d) Menyediakan khidmat nasihat perundangan bagi melindungi aset ICT, sumber dan kakitangan jabatan terhadap pelbagai risiko perundangan;
2.7 Pengurus Sumber Manusia	
	<ul style="list-style-type: none"> a) Memaklumkan dasar, polisi, pekeliling dan garis panduan pengurusan sumber manusia berkaitan dengan ICT; b) Menyediakan khidmat sokongan pentadbiran bagi urusan menyimpan dan menyelenggarakan maklumat pengurusan sumber manusia berkaitan dengan ICT dengan mematuhi peraturan, undang-undang dan polisi yang berkuat kuasa; c) Memaklumkan sebarang pertukaran, perpindahan, persaraan dan atau penamatan perkhidmatan kakitangan kepada pentadbir sistem ICT; d) Menyelaras urusan tatatertib dan perkhidmatan sumber manusia; dan e) Menghebahkan dasar, polisi, pekeliling dan garis panduan yang berkaitan dengan perjawatan, penilaian prestasi, kemajuan kerjaya, skim gaji dan perkara-perkara lain yang berkaitan dengan perjawatan.

Bil.	Perkara
2.8 Pihak Ketiga	
	<ul style="list-style-type: none"> a) Menjaga kerahsiaan maklumat berkaitan penggunaan ICT; 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 BPM; dan d) Mendapatkan kelulusan untuk menggunakan kemudahan ICT.
2.9 Pengguna Peranti mobil and <i>teleworking</i>	
	<ul style="list-style-type: none"> a) Pengguna Peranti mudah alih milik persendirian Pengguna peranti mudah alih milik persendirian hendaklah dikawal daripada mencapai maklumat Rahsia Rasmi dan hendaklah mematuhi polisi serta prosedur yang ditetapkan untuk dibawa masuk ke kawasan terperingkat. b) Pengguna <i>Teleworking</i> <ul style="list-style-type: none"> i. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; ii. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan iii. Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT.

BAB 3: KESELAMATAN SUMBER MANUSIA

Objektif: Memastikan semua pihak yang terlibat dalam pengurusan dan penggunaan ICT hendaklah:

1. Memahami tanggungjawab dan peranan;
2. Meningkatkan pengetahuan dan kesedaran; dan
3. Menguruskan aspek keselamatan siber secara teratur

Dalam meningkatkan keselamatan penyampaian maklumat dan mengurangkan risiko penyalahgunaan aset ICT semua pihak terlibat hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

Bil.	Perkara	Tanggungjawab
3.1 Sebelum Dalam Perkhidmatan		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: <ol style="list-style-type: none"> a) Menjelaskan peranan dan tanggungjawab pihak yang terlibat dalam meningkatkan keselamatan penyampaian maklumat dan mengurangkan risiko penyalahgunaan aset 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/ Pengguna/ Pihak Ketiga
3.2 Semasa Dalam Perkhidmatan		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: <ol style="list-style-type: none"> a) Memastikan pihak terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan; 	ICTSO/ Pengurus ICT/ Pengurus Sumber Manusia/ Pengguna/ Pihak Ketiga

Bil.	Perkara	Tanggungjawab
	<p>b) Memastikan pihak yang terlibat mematuhi keselamatan siber berdasarkan kepada dasar dan peraturan yang ditetapkan oleh Kerajaan;</p> <p>c) Memastikan tindakan disiplin atau undang-undang dilaksanakan sekiranya berlaku pelanggaran peraturan yang ditetapkan;</p> <p>d) Memastikan tanggungjawab dan peranan dalam pengurusan keselamatan siber dinyatakan dalam senarai tugas yang merangkumi:</p> <p>i. Tanggungjawab kakitangan;</p> <p>ii. Hubungan dengan pegawai atasan; dan</p> <p>iii. Tanggungjawab kakitangan dalam keselamatan siber.</p> <p>e) Kakitangan haruslah diberi latihan yang bersesuaian dan berterusan dalam semua aspek keselamatan siber yang berkaitan dengan tugas mereka;</p> <p>f) Kakitangan bertanggungjawab mengikuti latihan pengurusan keselamatan siber berdasarkan keperluan;</p> <p>g) PB bertanggungjawab mengkaji semula keperluan latihan untuk setiap kakitangan di bawahnya; dan</p> <p>h) Program kesedaran keselamatan siber juga perlu dilaksanakan secara berterusan sebagai langkah peringatan kepada kakitangan jabatan berkenaan kepentingan keselamatan aset ICT jabatan.</p>	
3.3 Bertukar/ Tamat Perkhidmatan/ Cuti Belajar		
	<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a) Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan atau terma perkhidmatan yang ditetapkan; dan</p>	<p>ICTSO/ Pentadbir Sistem/ Pengguna/ Pihak Ketiga</p>

Bil.	Perkara	Tanggungjawab
	b) Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.	

BAB 4: PENGURUSAN ASET

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

Bil.	Perkara	Tanggungjawab
4.1 Tanggungjawab Terhadap Aset		
4.1.1	Inventori dan Pemilikan Aset ICT	
	<p>Semua aset ICT di jabatan mestilah diuruskan mengikut peraturan dan tatacara yang berkuat kuasa seperti berikut:</p> <ul style="list-style-type: none"> a) Setiap aset ICT hendaklah didaftarkan dan ditentukan pemiliknya. Pengarah Bahagian adalah bertanggungjawab mengenal pasti pemilik aset ICT tersebut; b) Pemilik aset hendaklah menentukan tahap sensitiviti (terperingkat) yang bersesuaian bagi setiap maklumat aset di jabatan. Pemilik aset juga hendaklah membuat keputusan dalam menentukan individu yang dibenarkan untuk capaian dan penggunaan maklumat tersebut; c) Pentadbir aset ICT adalah bertanggungjawab untuk menentukan prosedur kawalan khas (contohnya: kawalan capaian), kaedah pelaksanaan dan penyelenggaraan serta menyediakan langkah pemulihan yang konsisten dengan arahan pemilik aset; d) Semua pengguna aset ICT mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh pemilik aset atau pentadbir sistem. Pengguna adalah terdiri daripada kakitangan jabatan (lantikan tetap, pinjaman, kontrak dan sambilan), konsultan, kontraktor atau pihak ketiga yang terlibat secara langsung; e) Kehilangan/ kecurian aset ICT mestilah dilaporkan serta merta mengikut prosedur pengurusan 	<p>PB/ Pentadbir Aset ICT/ Pemilik Aset/ Pengguna Aset</p>

Bil.	Perkara	Tanggungjawab
	<p>kehilangan/ kecurian aset berpandukan Arahan Perbendaharaan yang telah ditetapkan;</p> <p>f) Senarai maklumat aset di jabatan hendaklah diwujudkan. Setiap aset perlu ditentukan dengan jelas dan pemilikan aset mestilah dipersetujui dan didokumenkan berserta lokasi semasa aset tersebut. Senarai aset hendaklah disimpan oleh pengarah bahagian atau Pentadbir Aset ICT Jabatan; dan</p> <p>g) Setiap pengguna adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan aset ICT di bawah tanggungannya.</p>	
4.1.2	Peralatan Mudah Alih dan Kerja Jarak Jauh	
	<p>Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti berikut:</p> <p>a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;</p> <p>b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat;</p> <p>c) Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT;</p> <p>d) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan</p> <p>e) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.</p>	PB/Pentadbir Aset ICT/Pemilik Aset/ Pengguna Aset

Bil.	Perkara	Tanggungjawab
4.1.3	Peminjaman dan Pemulangan Aset ICT	
	<p><u>Peminjaman</u> Langkah-langkah perlu diambil termasuklah seperti berikut:</p> <ol style="list-style-type: none"> a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh jabatan bagi membawa keluar peralatan bagi tujuan yang dibenarkan; b) Melindungi dan mengawal peralatan sepanjang masa; c) Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan d) Menyemak peralatan ketika peminjaman dan pemulangan dilakukan. <p><u>Pemulangan</u> Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan atau terma perkhidmatan yang ditetapkan bagi pegawai yang :</p> <ol style="list-style-type: none"> a) Bertukar keluar; b) Bersara; c) Ditamatkan perkhidmatan; dan d) Diarahkan oleh Pengarah Bahagian <p>Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.</p>	PB/Pentadbir Aset ICT/Pemilik Aset/Pengguna Aset

Bil.	Perkara	Tanggungjawab
4.2 Pengelasan, Pelabelan dan Pengendalian Maklumat		
4.2.1	Pengelasan Maklumat	
	<p>Pengelasan maklumat bertujuan memastikan setiap maklumat diberi perlindungan oleh pemilik aset untuk menentukan keperluan, keutamaan dan tahap keselamatan berdasarkan peraturan yang berkuat kuasa seperti berikut:</p> <p>Rahsia Besar;</p> <p>a) Rahsia;</p> <p>b) Sulit;</p> <p>c) Terhad; dan</p> <p>d) Data Terbuka.</p>	PB/ Pentadbir Aset ICT/ Pemilik Aset/ Pengguna Aset
4.2.2	Pelabelan dan Pengendalian Maklumat	
	<p>Semua maklumat mestilah dilabelkan mengikut klasifikasi maklumat seperti yang dinyatakan pada para 4.2.1 Pengelasan Maklumat.</p> <p>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</p> <p>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 jabatan atas dasar perlu tahu sahaja dan mestilah mendapat kebenaran daripada jabatan.</p>	Pentadbir Aset/ Pemilik Aset
4.3 Pengendalian Media Penyimpanan Maklumat		
	<p>Perkara-perkara yang mesti dipatuhi adalah seperti berikut:</p> <p>a) Memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan aset</p>	Pentadbir Aset/ Pemilik Aset

Bil.	Perkara	Tanggungjawab
	<p>secara tidak sah, yang boleh mengganggu aktiviti perkhidmatan;</p> <p>b) Prosedur perlu disediakan untuk pengurusan peralatan penyimpanan maklumat mudah alih;</p> <p>c) Peralatan penyimpanan maklumat yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan;</p> <p>d) Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna;</p> <p>e) Dokumentasi sistem perlu dilindungi daripada capaian yang tidak dibenarkan;</p> <p>f) Polisi, prosedur dan kawalan pertukaran maklumat yang rasmi perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi dalam agensi dan mana-mana pihak terjamin;</p> <p>g) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara agensi dengan pihak luar;</p> <p>h) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari agensi;</p> <p>i) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan</p> <p>j) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat agensi.</p>	

Bil.	Perkara	Tanggungjawab
4.4 Kawalan Membawa Peranti Anda Sendiri (BYOD)		
	<p>Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD seperti berikut:</p> <ol style="list-style-type: none"> a) Semua peringkat maklumat rasmi kerajaan adalah hakmilik kerajaan; b) Sebarang bahan rasmi yang dimuatnaik/ edar/ kongsi hendaklah mendapat kebenaran Pengarah Bahagian; c) Menandatangani Surat Akuan Pematuhan PKS dan Akta Rahsia Rasmi 1972 [Akta 88]; d) Memastikan peranti yang digunakan mempunyai kawalan keselamatan seperti berikut: <ol style="list-style-type: none"> i. Menetapkan mekanisme kawalan akses bagi BYOD dan akan mengunci secara automatik apabila tidak digunakan; ii. Melaksanakan penyulitan dan/atau perlindungan ke atas folder yang mempunyai maklumat rasmi Kerajaan yang disimpan di dalam peranti BYOD; dan iii. Memastikan BYOD mempunyai ciri-ciri keselamatan standard seperti antivirus, patching terkini dan <i>anti theft</i>. e) Pengguna adalah dilarang daripada melakukan perkara berikut: <ol style="list-style-type: none"> i. Menyimpan maklumat rasmi di dalam BYOD; ii. Menggunakan BYOD untuk mengakses, menyimpan dan menyebarkan maklumat rasmi dan terperingkat kepada pihak yang tidak dibenarkan; 	Pemilik Aset

Bil.	Perkara	Tanggungjawab
	<p>iii. Menjadikan BYOD sebagai medium sandaran (backup) bagi maklumat rasmi;</p> <p>iv. Merakam komunikasi dan dokumen rasmi untuk tujuan peribadi; dan</p> <p>v. Menjadikan BYOD sebagai <i>access point</i> kepada aset ICT jabatan untuk capaian ke Internet tanpa kebenaran.</p> <p>Pengguna adalah tertakluk kepada perkara seperti berikut:</p> <p>a) Menggunakan BYOD secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/dasar yang berkuat kuasa;</p> <p>b) Memadamkan segala maklumat yang berkaitan dengan urusan rasmi jabatan sekiranya bertukar/ditamatkan perkhidmatan/bersara ATAU sewaktu dihantar ke pusat servis untuk penyelenggaraan;</p> <p>c) Bertanggungjawab dan boleh dikenakan tindakan tatatertib sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/ kerosakan/ pendedahan maklumat rasmi Kerajaan;</p> <p>d) JWP berhak merampas mana-mana BYOD pengguna sekiranya didapati atau disyaki tidak mematuhi peraturan yang telah ditetapkan; dan</p> <p>e) JWP tidak bertanggungjawab atas kehilangan, kerosakan data atau aplikasi dalam BYOD yang digunakan untuk tujuan urusan rasmi jabatan.</p>	

BAB 5: PENGURUSAN KAWALAN CAPAIAN

Objektif: Mengawal Capaian Maklumat

Bil.	Perkara	Tanggungjawab
5.1 Keperluan Kawalan Capaian		
	<p>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 dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a) Kawalan capaian ke atas aset 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. 	<p>Pentadbir Rangkaian/ Pentadbir Sistem/Pengguna</p>
5.2 Kawalan Capaian Rangkaian		
	<p>Polisi akses kepada rangkaian dan servis rangkaian yang konsisten dengan polisi kawalan capaian perlu diwujudkan dan merangkumi:</p> <ol style="list-style-type: none"> a) Rangkaian dan servis rangkaian yang diberikan kebenaran akses sahaja; b) Prosedur penentuan pengguna yang diberi akses; c) Pengurusan kawalan dan prosedur untuk melindungi rangkaian; d) Keperluan pengesahan pengguna untuk akses kepada servis rangkaian; dan e) Pemantauan penggunaan servis rangkaian. 	<p>Pentadbir Rangkaian/ Pentadbir Sistem/ Pengguna</p>

Bil.	Perkara	Tanggungjawab
5.3 Pengurusan Capaian Pengguna		
	<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a) Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan; b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat; c) Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan; d) Pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan jabatan dan tindakan pengemaskinian dan atau pembatalan hendaklah diambil atas sebab seperti berikut: <ol style="list-style-type: none"> i. Pengguna tidak hadir bertugas tanpa kebenaran melebihi dari tujuh (7) hari; ii. Pengguna bercuti atau bertugas di luar pejabat mengikut peraturan yang berkuat kuasa; iii. Pengguna bertukar jawatan, tanggungjawab dan atau bidang tugas. Pembatalan akan dilakukan di hari terakhir pertukaran tersebut; iv. Pengguna yang sedang dalam prosiding dan atau dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib. Pembatalan akan dilakukan serta merta apabila dimaklumkan oleh pihak yang mengendalikan pengurusan sumber manusia; dan v. Pengguna bertukar, berpindah, bersara dan atau tamat perkhidmatan. Pembatalan akan dilakukan berdasarkan tarikh arahan yang dikeluarkan oleh Bahagian Khidmat Pengurusan (BKP). 	<p>Pentadbir Rangkaian/ Pentadbir Sistem/ Pengguna</p>

Bil.	Perkara	Tanggungjawab
	<p>e) Aktiviti capaian oleh pengguna direkod dan diselenggarakan dengan sistematik dari semasa ke semasa. Maklumat yang di rekod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya; dan</p> <p>f) Akaun pengguna yang baru diwujudkan perlu diberikan kata laluan sementara dan pengguna perlu menukar kata laluan apabila log masuk dibuat pada kali pertama.</p>	
5.4 Kawalan Capaian Sistem dan Aplikasi		
	<p>Kawalan capaian sistem dan aplikasi perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan.</p> <p>a) Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:</p> <ul style="list-style-type: none"> i. Menyediakan kaedah yang sesuai untuk pengesahan capaian (<i>authentication</i>); dan ii. Mengehadkan tempoh penggunaan mengikut kesesuaian. <p>b) Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> i. Menamatkan sesuatu sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan; dan ii. Mengehadkan tempoh sambungan ke sesuatu aplikasi berisiko tinggi. <p>c) Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> i. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan 	Pentadbir ICT/ Pengguna

Bil.	Perkara	Tanggungjawab
	<p>mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;</p> <p>ii. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);</p> <p>iii. Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;</p> <p>iv. Menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat;</p> <p>v. Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem maklumat terperingkat (sulit/ rahsia); dan</p> <p>vi. Pengguna digalakkan membuat enkripsi dengan menukarkan teks biasa (<i>plain text</i>) kepada bentuk <i>cipher text</i> ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.</p>	
5.5 Pengurusan Kata Laluan		
	<p>Sistem pengurusan kata laluan perlu:</p> <p>a) Memastikan penggunaan ID pengguna dan kata laluan tidak dikongsi;</p> <p>b) Membenarkan pengguna menukar kata laluan sendiri;</p> <p>c) Menekankan pilihan kata laluan yang berkualiti;</p> <p>d) Mewajibkan pengguna menukar kata laluan apabila log masuk kali pertama;</p> <p>e) Menyimpan rekod bagi kata laluan terdahulu dan mengelakkan penggunaan kata laluan yang berulang;</p> <p>f) Tidak memaparkan kata laluan di skrin ketika log masuk;</p> <p>g) Menyimpan kata laluan di dalam fail yang berasingan dengan fail data aplikasi; dan</p>	<p>Pentadbir ICT/Pengguna</p>

Bil.	Perkara	Tanggungjawab
	h) Mewajibkan pengguna menukar kata laluan sekurang-kurangnya setiap tiga (3) bulan untuk ke semua sistem utama.	
5.6 Tanggungjawab Pengguna		
	<p>Pengguna perlu mematuhi amalan terbaik penggunaan kata laluan seperti berikut:</p> <ul style="list-style-type: none"> a) Pengguna 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 <i>root ID</i> dan kata laluan bagi sistem utama. Di dalam hal ini, kata laluan haruslah dilindungi dengan menggunakan mekanisme kawalan lain seperti menyimpan kata laluan di dalam laci berkunci dan menggunakan kata laluan yang berbeza bagi capaian berbeza; b) Pengguna adalah tidak digalakkan mengguna kata laluan yang sama bagi kegunaan sistem di jabatan mahupun sistem yang tidak terdapat di jabatan; c) Pengguna hendaklah tidak mendedahkan kata laluan yang diguna pakai di jabatan kepada sesiapa. Ini termasuklah ahli keluarga dan bukan ahli keluarga apabila melakukan kerja pejabat di rumah. Walau bagaimana pun, bagi ID kata laluan utama yang disimpan di dalam laci berkunci, harus diadakan satu proses mengenai tatacara memperoleh kata laluan berkenaan sekiranya berlaku ketidakhadiran pemegang kata laluan utama sewaktu ia diperlukan; d) Pengguna haruslah menyimpan kata laluan dengan selamat dan tidak dibenarkan berkongsi akaun dengan pengguna lain. Pengguna yang disahkan adalah bertanggungjawab ke atas kerahsiaan dan keselamatan kata laluan dan akaun mereka; 	Pengguna

Bil.	Perkara	Tanggungjawab
	<p>e) Penggunaan atribut <i>Remember Me</i> adalah tidak dibenarkan sama sekali. Sekiranya akaun atau kata laluan disyaki telah dicerobohi, maka laporan kejadian hendaklah dilaporkan kepada pasukan tindak balas insiden keselamatan siber [<i>Cyber Security Incident Response Team (CSIRT)</i>] jabatan dan tindakan menukar kata laluan perlu dilakukan;</p> <p>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</p> <p>g) Sistem pengurusan kata laluan hendaklah menekankan pilihan kata laluan yang berkualiti. Kata laluan yang berkualiti antara lain mempunyai ciri-ciri seperti berikut:</p> <ul style="list-style-type: none"> i. Gabungan minimum dua belas (12) aksara yang mengandungi kombinasi antara huruf, nombor dan simbol (seperti: 0-9, a-z, A-Z, ! @ # \$ % ^ & * () - +); dan ii. Kata laluan yang ditentukan oleh pengguna hendaklah tidak digunakan semula. Pengguna 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 data, jaminan pengesahan sumber data, tanpa-sangkalan dan jaminan pengesahan entiti.

Bil.	Perkara	Tanggungjawab
6.1 Kriptografi		
	<p>Kriptografi bermaksud sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.</p> <p>Tindakan melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi yang boleh dilakukan adalah seperti berikut:</p> <ol style="list-style-type: none"> a) Penggunaan enkripsi dengan menukarkan teks biasa (<i>plain text</i>) kepada bentuk <i>cipher text</i> ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa; b) Penggunaan fungsi <i>hash</i> dan Kod Pengesahan Mesej (MAC) c) Penggunaan tandatangan digital digalakkan kepada semua pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; d) Pengurusan ke atas <i>Public Key Infrastructure</i> (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. 	Pemilik aset/ Pengguna aset

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 Fizikal		
7.1.1	Keselamatan Fizikal	
	<p>Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh premis.</p> <p>Langkah-langkah keselamatan fizikal adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 keluar masuk; f) Mengadakan kaunter kawalan; g) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; h) Mewujudkan perkhidmatan kawalan keselamatan; i) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang mendapat kebenaran sahaja untuk masuk; j) Merekabentuk dan melaksanakan perlindungan fizikal daripada bencana seperti kebakaran, banjir, letupan atau huru hara; 	CGSO/ Pegawai Keselamatan/ CIO/ ICTSO

Bil.	Perkara	Tanggungjawab
	k) Menyediakan garis panduan keselamatan untuk kakitangan yang bekerja di dalam kawasan terhad; l) Sistem kawalan kunci dengan menetapkan pegawai yang bertanggungjawab untuk menyimpan kunci dengan baik dan mempunyai rekod; dan m) Mewujudkan kawalan di kawasan penghantaran, pemunggaran dan kawasan larangan.	
7.1.2	Kawalan Masuk Fizikal	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna hendaklah memakai pas keselamatan sepanjang waktu bertugas; b) Setiap pelawat mestilah mendaftar dan mendapatkan pas pelawat di pintu masuk utama jabatan untuk ke kawasan/tempat berurusan dan hendaklah dikembalikan semula selepas tamat urusan; c) Semua pas keselamatan hendaklah diserahkan semula kepada jabatan apabila pengguna bertukar, berhenti atau bersara; dan d) Kehilangan pas keselamatan mestilah dilaporkan dengan segera kepada pegawai keselamatan jabatan.	Pengguna/ Pelawat

Bil.	Perkara	Tanggungjawab
7.1.3	Kawasan Larangan	
	<p>Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di jabatan adalah di Bilik Pusat Data, Bilik Fail dan lain-lain.</p> <p>a) Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja;</p> <p>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;</p> <p>c) Semua aktiviti pihak ketiga di kawasan larangan perlu mendapat kebenaran daripada pegawai yang diberi kuasa dan dipantau serta dikawal oleh pegawai bertanggungjawab;</p> <p>d) Peralatan/ media perakaman/ storan/ komunikasi adalah tidak dibenarkan dibawa masuk ke dalam pusat data; dan</p> <p>e) Aktiviti mengambil gambar, merakam video, merekodkan suara atau penggunaan peralatan yang tidak berkenaan adalah dilarang.</p>	ICTSO/ Pengguna/ Pihak Ketiga/ Pelawat
7.2 Keselamatan Peralatan ICT Dan Maklumat		
	Melindungi peralatan ICT dan maklumat dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
7.2.1	Peralatan ICT	
	Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan dengan mengambil tindakan berikut:	Pengguna, Pentabir Sistem ICT/ Pihak Ketiga, ICTSO/ pegawai aset

Bil.	Perkara	Tanggungjawab
	<p>a) Pengguna mesti mendapat kebenaran daripada ICTSO atau pegawai yang diberikan kuasa untuk membuat instalasi perisian tambahan;</p> <p>b) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (<i>activated</i>) dan dikemaskini disamping melakukan imbasan ke atas media storan yang digunakan;</p> <p>c) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;</p> <p>d) Peralatan-peralatan kritikal perlu disokong oleh <i>Uninterruptable Power Supply (UPS)</i>;</p> <p>e) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (<i>air ventilation</i>) yang sesuai;</p> <p>f) Peralatan ICT yang hendak dibawa keluar dari premis jabatan untuk tujuan rasmi, perlu mendapat kelulusan pegawai yang diberikan kuasa dan direkodkan bagi tujuan pemantauan;</p> <p>g) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;</p> <p>h) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;</p> <p>i) Pengguna mesti mendapat kebenaran daripada ICTSO atau pegawai yang diberikan kuasa untuk mengubah kedudukan komputer dari tempat asal;</p> <p>j) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada pegawai yang bertanggungjawab untuk dibaik pulih;</p> <p>k) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;</p>	

Bil.	Perkara	Tanggungjawab
	<p>l) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;</p> <p>m) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir Sistem ICT;</p> <p>n) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;</p> <p>o) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat;</p> <p>p) Memastikan plug dicabut daripada suis utama (<i>main switch</i>) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya;</p> <p>Semua pihak yang terlibat dalam pengurusan atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut:</p> <p>a) Memastikan semua aset ICT dikembalikan mengikut peraturan dan terma yang ditetapkan; dan</p> <p>b) Membatalkan atau menarik balik semua kebenaran, capaian ke atas aset ICT mengikut peraturan yang ditetapkan.</p>	
7.2.2	Media Storan	
	<p>Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, <i>optical disk</i>, <i>flash disk</i>, <i>thumb drive</i>, <i>external drive</i> dan media storan lain. Media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.</p>	Pengguna/ Pentadbir Sistem ICT

Bil.	Perkara	Tanggungjawab
	<p>Tindakan berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan adalah terjamin dan selamat:</p> <ul style="list-style-type: none"> a) Sediakan ruang penyimpanan yang kondusif dan selamat serta bersesuaian 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 untuk tujuan pinjaman; e) Mendapat kelulusan pemilik maklumat terlebih dahulu sebelum menghapuskan maklumat atau kandungan media storan dengan teratur dan selamat; f) 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; g) Mengadakan salinan atau penduaan (<i>backup</i>) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h) Perkakasan penduaan (<i>backup</i>) hendaklah diletakkan di tempat yang terkawal; dan i) Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan. 	
7.2.3	Media Tandatangan Digital	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pengguna/ Pentadbir Sistem ICT

Bil.	Perkara	Tanggungjawab
	a) Pengguna 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 pegawai yang bertanggungjawab untuk tindakan seterusnya.	
7.2.4	Media Perisian dan Aplikasi	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan jabatan; b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c) Lesen perisian (<i>registration code</i> , 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) <i>Source code</i> sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	ICTSO/ Pentabir Sistem/ Pengguna
7.2.5	Penyelenggaraan peralatan ICT	
	Peralatan ICT hendaklah diselenggarakan dengan baik bagi memastikan kerahsiaan, integriti dan kebolehsediaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;	Pengguna/ Pentabir Sistem/ Pihak Ketiga

Bil.	Perkara	Tanggungjawab
	c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
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 jabatan bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; b) Pengguna perlu melindungi dan mengawal peralatan sepanjang tempoh pinjaman; c) Memastikan aktiviti pinjaman dan pemulangan peralatan ICT direkodkan; dan d) Memastikan peralatan ICT yang dipulangkan dalam keadaan baik dan lengkap.	Pengguna/ Pentabir Sistem/ Pihak Ketiga
7.2.7	Peralatan ICT di Luar Premis Jabatan	
	Bagi peralatan ICT yang dibawa keluar dari premis jabatan, 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	Pengguna/ Pegawai Aset/ Pihak ketiga

Bil.	Perkara	Tanggungjawab
	Kerajaan. Maklumat perlu dihapuskan dari peralatan tersebut setelah disalin ke media storan sekunder.	
7.2.8	Pelupusan Peralatan Aset ICT	
	<p>Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa mengikut Tatacara Pengurusan Aset Alih Kerajaan. Pelupusan peralatan ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan jabatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a) Semua kandungan peralatan ICT khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilaksanakan; dan</p> <p>b) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat.</p>	Pegawai Aset/ Pengguna
7.2.9	Clear Desk dan Clear Screen	
	Semua maklumat dalam apa jua bentuk media storan hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. <i>Clear Desk</i> dan <i>Clear Screen</i> bermaksud tidak meninggalkan bahan-bahan yang sensitif dan terperingkat terdedah sama ada di atas meja atau di paparan skrin apabila pemilik tidak berada di tempatnya. Langkah yang perlu diambil adalah dengan menggunakan kemudahan <i>password screensaver</i> , <i>lock PC</i> atau log keluar apabila meninggalkan komputer.	Pengguna
7.3 Keselamatan Persekitaran		
	Melindungi aset ICT dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.	
7.3.1	Kawalan Persekitaran	
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa dan	ICTSO/ Bahagian Pentadbiran

Bil.	Perkara	Tanggungjawab
	<p>mengubahsuai hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> a) Merancang dan menyediakan pelan keseluruhan susun atur peralatan komputer, 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) Peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dicapai dan dikendalikan; d) Bahan mudah terbakar DILARANG disimpan di dalam kawasan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna adalah DILARANG merokok atau menggunakan peralatan memasak seperti cerek elektrik, ketuhar gelombang mikro dan lain-lain berhampiran peralatan PC; 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) Akses kepada bilik sesalur telefon hendaklah sentiasa dikunci; dan 	

Bil.	Perkara	Tanggungjawab
	i) Mematuhi peraturan yang telah ditetapkan oleh pihak berkuasa seperti Jabatan Bomba dan Penyelamat, Jabatan Kerja Raya dan sebagainya.	
7.3.2	Bekalan Kuasa	
	<p>Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan hendaklah disalurkan mengikut voltage yang bersesuaian;</p> <p>b) Peralatan sokongan seperti <i>Uninterruptable Power Supply</i> (UPS) dan penjana (<i>generator</i>) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan</p> <p>c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.</p>	ICTSO/ Penyelenggara Bangunan
7.3.3	Kabel Peralatan ICT	
	<p>Kabel peralatan ICT hendaklah dilindungi kerana ia adalah salah satu punca maklumat. Langkah-langkah keselamatan kabel adalah seperti berikut:</p> <p>a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;</p> <p>b) Melindungi kabel dengan menggunakan conduit untuk mengelakkan kerosakan yang disengajakan atau tidak disengajakan;</p> <p>c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan <i>wire tapping</i>; dan</p> <p>d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.</p>	ICTSO/ Pentadbir Sistem/ Bahagian Pentadbiran

Bil.	Perkara	Tanggungjawab
7.3.4	Prosedur Kecemasan	
	<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang telah ditetapkan; b) Melaporkan insiden kecemasan persekitaran kepada Pegawai Keselamatan; dan c) Mengadakan, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa; 	ICTSO
7.4 Keselamatan Dokumen		
	Melindungi maklumat dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaiian.	
7.4.1	Dokumen	
	<p>Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> a) Memastikan sistem dokumentasi atau penyimpanan dokumen adalah selamat dan kehilangan atau kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; b) Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; c) Pergerakan fail terperingkat dan dokumen rahsia rasmi hendaklah mengikut prosedur keselamatan; d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; e) Dokumen terperingkat rasmi perlu dienkrripsikan sebelum dihantar secara elektronik; dan f) Memastikan cetakan yang mengandungi maklumat terperingkat diambil segera dari pencetak. 	ICTSO

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		
	Memastikan pengurusan operasi pemprosesan maklumat dilaksanakan dengan cekap dan selamat.	
8.1.1	Pengendalian Prosedur Operasi	
	<p>Semua prosedur pengurusan operasi hendaklah dikenal pasti, didokumenkan, disimpan dan dihadkan capaian berdasarkan keperluan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> a) Semua prosedur operasi hendaklah didokumenkan dengan jelas, teratur, dikemaskinikan dan sedia diguna pakai oleh pengguna; b) Setiap perubahan kepada prosedur operasi mestilah dikawal; c) Tugas dan tanggungjawab fungsi perlu diasingkan bagi mengurangkan risiko kecuaiian dan penyalahgunaan aset ICT; 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

Bil.	Perkara	Tanggungjawab
8.1.2	Pengurusan Perubahan	
	<p>Perubahan kepada organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang memberi kesan kepada keselamatan maklumat hendaklah dikawal.</p> <p>Pengurusan ke atas perubahan perlu diambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a) Mewujudkan prosedur pengurusan perubahan; b) Merekodkan semua perubahan yang telah dipersetujui dan dilaksanakan; dan c) Memantau pelaksanaan perubahan. 	ICTSO/Pengguna/ Pentadbir Sistem
8.1.3	Pengurusan Kapasiti	
	<p>Kapasiti sistem ICT hendaklah dirancang, diurus dan dikawal dengan terperinci bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan operasi sistem ICT.</p> <p>Keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.</p>	ICTSO/ Pentadbir Sistem
8.1.4	Pengasingan Kemudahan Pembangunan, Ujian dan Operasi	
	<p>Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian ataupun perubahan tidak sah ke atas persekitaran operasi.</p> <p>Perkara-perkara yang perlu dipatuhi:</p> <ol style="list-style-type: none"> a) Mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan operasi; b) Merekodkan semua penggunaan sumber yang dilaksanakan; dan 	ICTSO/ Pentadbir Sistem

Bil.	Perkara	Tanggungjawab
	c) Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.	
8.2 Perlindungan daripada <i>Malware</i>		
8.2.1	Aset ICT perlu dilindungi supaya tidak terdedah kepada kerosakan yang disebabkan oleh kod berbahaya seperti <i>virus</i> , <i>worm</i> , <i>trojan</i> dan lain-lain.	
8.2.2	<p>Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi sistem ICT daripada gangguan <i>malicious code</i></p> <p>Perkara-perkara yang mesti dipatuhi adalah:</p> <ul style="list-style-type: none"> a) Memasang sistem keselamatan untuk mengesan perisian berbahaya seperti antivirus, <i>Intrusion Detection System (IDS)</i> dan <i>Intrusion Prevention System (IPS)</i>; b) Mengimbas semua perisian dengan antivirus sebelum menggunakannya; c) Mengemaskinikan paten antivirus dari semasa ke semasa; d) Memasang dan menggunakan hanya perisian yang tulen; e) Menyemak kandungan sistem ICT secara berkala bagi mengesan aktiviti yang tidak normal seperti manipulasi data tidak sah yang menyebabkan pertambahan, perubahan, kehilangan atau kerosakan maklumat; f) Memasukkan klausa tanggungan ke dalam kontrak yang ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; g) Mewujud dan melaksanakan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; h) Memberi amaran mengenai ancaman seperti serangan virus terhadap keselamatan aset ICT jabatan; i) Menghadiri program kesedaran mengenai ancaman 	ICTSO/ Pentadbir Sistem/ Pegguna

Bil.	Perkara	Tanggungjawab
	<p>perisian berbahaya dan cara mengendalikannya dari semasa ke semasa;</p> <p>j) Melaksanakan Program Kesedaran Pengguna yang bersesuaian; dan</p> <p>k) Penggunaan <i>mobile code</i> yang boleh mendatangkan ancaman keselamatan siber adalah tidak dibenarkan.</p>	
8.3 Backup		
8.3.1	Memastikan kesinambungan perkhidmatan berjalan lancar	
8.3.2	<p>Salinan pendua maklumat dan perisian sistem hendaklah disediakan dan diuji secara berkala selaras dengan polisi <i>backup</i> bagi tujuan kesinambungan operasi pemprosesan maklumat.</p> <p>Perkara-perkara yang mesti dipatuhi adalah seperti berikut:</p> <p>a) Membuat salinan pendua ke atas semua maklumat dan sistem perisian mengikut jadual yang ditetapkan atau apabila berlaku perubahan versi;</p> <p>b) Menyimpan salinan pendua di lokasi lain yang selamat; dan</p> <p>c) Menguji sistem pendua bagi memastikan ianya dapat beroperasi dengan normal.</p>	Pentadbir Sistem
8.4 Log dan Pemantauan		
8.4.1	Semua peristiwa dan bukti kewujudan insiden hendaklah direkodkan untuk tujuan jejak audit.	
8.4.2	<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a) Setiap sistem mestilah mempunyai jejak audit;</p> <p>b) Mewujudkan prosedur untuk memantau penggunaan kemudahan memproses maklumat dan dipantau secara berkala;</p> <p>c) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;</p>	ICTSO/ Pentadbir Sistem

Bil.	Perkara	Tanggungjawab
	<p>d) Maklumat log perlu dilindungi daripada sebarang ubahsuai dan capaian yang tidak dibenarkan;</p> <p>e) Sebarang kesalahan, kesilapan atau penyalahgunaan sistem perlu direkodkan, dianalisis dan diambil tindakan sewajarnya;</p> <p>f) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera;</p> <p>g) Waktu yang berkaitan dengan sistem pemrosesan maklumat perlu diselaraskan dengan satu sumber waktu yang piawai; dan</p> <p>h) Sebarang aktiviti tidak sah seperti kecurian maklumat dan pencerobohan hendaklah dilaporkan kepada pasukan tindak balas insiden keselamatan siber [(<i>Cyber Security Incident Response Team (CSIRT)</i>)].</p>	
8.5 Kawalan Pengoperasian Perisian		
	<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan jabatan; dan</p> <p>b) Lesen perisian (<i>registration code, CD-keys, nombor siri dan langganan atas talian</i>) perlu disimpan berasingan daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak.</p>	Pentadbir Sistem
8.6 Pengurusan Kerentanan Teknikal		
8.6.1	Kawalan terhadap sebarang kelemahan teknikal pada perkakasan, sistem pengoperasian dan sistem aplikasi perlu diuruskan secara berkesan, sistematik dan berkala.	Pentadbir Sistem
8.6.2	<p>Perkara-perkara yang perlu dipatuhi adalah:</p> <p>a) Mengenal pasti maklumat keterdedahan teknikal sistem yang digunakan;</p> <p>b) Menilai tahap keterdedahan bagi mengenal pasti risiko</p>	ICTSO, Pentadbir Sistem

Bil.	Perkara	Tanggungjawab
	<p>yang bakal dihadapi; dan</p> <p>c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.</p>	
8.7 Pemakluman Audit		
	<p>a) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; dan</p> <p>b) Capaian ke atas sistem maklumat semasa pengauditan perlu dikawal selia bagi mengelakkan sebarang penyalahgunaan.</p>	Pentadbir Sistem

BAB 9: KESELAMATAN KOMUNIKASI

Objektif: Memastikan fasiliti rangkaian serta pengaliran maklumat dalam rangkaian dilindungi sepenuhnya.

Bil.	Perkara	Tanggungjawab
9.1 Pengurusan Keselamatan Rangkaian		
	Keselamatan rangkaian adalah elemen penting dalam memastikan pengaliran maklumat lancar dan sempurna.	
9.1.1	Kawalan Infrastruktur Rangkaian	
	<p>Infrastruktur rangkaian hendaklah dirancang, diurus dan dikawal bagi melindungi keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah:</p> <ul style="list-style-type: none"> a) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berkaitan dengan sistem rangkaian; b) Peralatan keselamatan seperti <i>firewall</i> hendaklah dipasang bagi memastikan hak capaian ke atas sistem dapat dilaksanakan seperti ditetapkan; c) Sebarang cubaan mencero boh dan aktiviti yang boleh mengancam sistem dan maklumat jabatan perlu dipantau dan dikesan melalui pemasangan peralatan keselamatan seperti <i>Intrusion Prevention System (IPS)</i>; 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 (<i>wireless</i>) LAN di jabatan hendaklah mematuhi peraturan yang dikeluarkan oleh pihak berkenaan seperti MAMPU dan Majlis Keselamatan Negara (MKN); dan g) Semua perisian berkaitan rangkaian dan keselamatan seperti <i>sniffer</i> atau <i>network analyzer</i> adalah dilarang 	ICTSO/ Pentadbir

Bil.	Perkara	Tanggungjawab
	dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.	
9.1.2	Keselamatan Perkhidmatan Rangkaian	
	<p>Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terjamin.</p> <p>Perkara-perkara yang perlu dipatuhi adalah:</p> <ul style="list-style-type: none"> a) Mekanisme keselamatan, tahap kesediaan 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 di bawah kawalan jabatan; dan c) Sebarang aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam (PKPA) yang berkuat kuasa perlu disekat melalui penggunaan <i>WebContent Filtering</i>. 	Pengguna/ Pentadbir Sistem
9.1.3	Pengasingan Rangkaian	
	<p>Pengasingan perkhidmatan rangkaian bertujuan untuk meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah:</p> <ul style="list-style-type: none"> a) Mengetahui pasti fungsi dan tanggungjawab pengguna; b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Mengemaskinikan hak capaian pengguna dari semasa ke semasa mengikut keperluan; dan 	Pentadbir

Bil.	Perkara	Tanggungjawab
	e) Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	
9.2 Pemindahan Maklumat		
	Memastikan keselamatan maklumat terjamin semasa pertukaran maklumat dengan entiti luar.	
9.2.1	Prosedur Pemindahan Maklumat	
	<p>Prosedur ini bertujuan untuk mengendali, menyimpan, memindah serta melindungi maklumat daripada didedah tanpa kebenaran atau salah guna serta memastikan keselamatan pemindahan maklumat dengan entiti luar terjamin.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> a) Mengehadkan dan menentukan capaian kepada pengguna yang dibenarkan sahaja; b) Mengehadkan pengedaran data untuk tujuan rasmi dan yang dibenarkan sahaja; c) Polisi, prosedur dan kawalan pemindahan maklumat yang formal perlu diwujudkan untuk melindungi pemindahan maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; d) Sebarang pemindahan maklumat di antara jabatan dan agensi lain mestilah dikawal; dan e) Penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi Kerajaan perlu mendapat kelulusan Pengarah Bahagian. 	ICTSO/ Pengguna/ Pentadbir Sistem
9.2.2	Perjanjian Pemindahan dan Kerahsiaan Maklumat	
	a) <i>Non-Disclosure Agreements</i> (NDA) perlu diwujudkan bagi memastikan kerahsiaan, integriti dan ketersediaan (CIA) maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara	Agensi/ Pentadbir/ Pihak ketiga/ Pengguna

Bil.	Perkara	Tanggungjawab
	jabatan dengan agensi luar dan b) Keperluan melindungi kerahsiaan meliputi integriti dan kerahsiaan maklumat hendaklah disemak secara berkala dan didokumenkan.	
9.2.3	Pengurusan Mesej Elektronik	
	Maklumat yang dihantar, diterima dan disimpan melalui mel elektronik perlu dilindungi bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan. Pengguna layak menerima kemudahan perkhidmatan emel dengan kelulusan dari Ketua Pengarah/Pengarah Bahagian.	PB/ Agensi/ Pentadbir Sistem/ Pengguna

BAB 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif : Memastikan sistem yang dibangunkan secara dalaman atau pun luaran mempunyai ciri-ciri keselamatan maklumat yang kukuh dan berdaya tahan daripada aktiviti berniat jahat serta merangkumi keseluruhan kitaran hayat aset.

Bil.	Perkara	Tanggungjawab
10.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat		
	<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan; b) Semua sistem 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 hendaklah mematuhi kawalan keselamatan. 	<p>JK Penilaian Teknikal/ JPICT/ Pentadbir Sistem/ Pembekal</p>
10.1.1 Perlindungan Perkhidmatan Aplikasi yang menggunakan Rangkaian Awam		
	<p>Maklumat aplikasi yang menggunakan rangkaian awam hendaklah dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat, pengubahsuaian maklumat yang tidak dibenarkan yang menyebabkan pertikaian kontrak.</p> <p>Perkara-perkara yang perlu dipatuhi adalah:</p> <ul style="list-style-type: none"> a) Identiti pengguna perlu dikenal pasti dan disahkan bagi menentukan tahap capaian maklumat yang dibenarkan; b) Setiap pengguna sistem perlu diberi peranan mengikut skop dan tanggungjawab yang ditetapkan; dan c) Memastikan pembekal diberi penjelasan dan menandatangani akuan pematuhan PKS mengenai 	<p>Pengurus ICT/ Pentadbir Sistem/ Pembekal</p>

Bil.	Perkara	Tanggungjawab
	keperluan mematuhi kontrak dan peraturan keselamatan yang ditetapkan.	
10.1.2	Melindungi Transaksi Perkhidmatan Atas Talian	
	<p>a) Maklumat yang terlibat dalam transaksi perkhidmatan atas talian hendaklah dilindungi daripada penghantaran yang tidak lengkap, <i>mis-routing</i>, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej; dan</p> <p>b) Kawalan terhadap keterdedahan perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.</p>	Pengurus ICT, Pentadbir Sistem
10.2 Keselamatan Dalam Proses Pembangunan Dan Sokongan		
	Memastikan keselamatan maklumat diwujudkan dan dilaksanakan dalam kitar hayat pembangunan sistem.	Pengurus ICT
10.2.1	Polisi Keselamatan Dalam Pembangunan Sistem	
	Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi dengan membangunkan Dokumen Pelan Pengurusan Keselamatan Maklumat atau <i>Information System Management Plan</i> (ISMP) semasa proses pembangunan sistem.	Pengurus ICT
10.2.2	Prosedur Kawalan Perubahan Sistem	
	<p>Prosedur kawalan perubahan hendaklah diwujudkan bagi mengawal sebarang perubahan terhadap sistem sepanjang kitar hayat pembangunan sistem.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a) Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang ditetapkan dan pelaksanaan hanya mengikut keperluan sahaja;</p>	Pengurus ICT, Pentadbir Sistem, Pemilik Sistem

Bil.	Perkara	Tanggungjawab
	<p>b) Perubahan atau pengubahsuaian ke atas perisian dan sistem hendaklah diuji, didokumenkan dan disahkan sebelum diguna pakai; dan</p> <p>c) Setiap perubahan kepada pengoperasian sistem perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan maklumat.</p>	
10.2.3 Semakan Teknikal Aplikasi Selepas Perubahan Platform		
	<p>Semakan dan pengujian terhadap aplikasi kritikal perlu dilaksanakan sekiranya berlaku perubahan terhadap platform pengoperasian bagi memastikan fungsi dan operasi sistem tidak terjejas.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a) Memastikan sistem aplikasi, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan; dan</p> <p>b) Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan.</p>	Pentadbir Sistem
10.2.4 Kawalan Terhadap Perubahan Kepada Perisian		
	Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.	Pentadbir Sistem
10.2.5 Prinsip Kejuruteraan Sistem Yang Selamat		
	Prinsip kejuruteraan keselamatan sistem hendaklah dibangunkan, didokumenkan, dikaji dan digunapakai ke atas semua pelaksanaan sistem maklumat.	Pentadbir Sistem
10.2.6 Persekitaran Pembangunan Sistem Yang Selamat		
	Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem.	Pentadbir Sistem

Bil.	Perkara	Tanggungjawab
	Secara umumnya kitar hayat pembangunan sistem termasuk skop dan objektif sistem, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian, penerimaan, pemasangan, konfigurasi, penyelenggaraan dan pelupusan.	
10.2.7	Pembangunan Sistem Secara Luaran	
	<p>Sebarang aktiviti pembangunan sistem yang melibatkan sumber luar perlu dikawal selia dan dipantau.</p> <p>Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut:</p> <ul style="list-style-type: none"> a) Memastikan spesifikasi perolehan mengandungi klausa tertentu berhubung keperluan keselamatan, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi pasukan pembangunan; b) Jabatan hendaklah memastikan <i>Intellectual property rights</i> (IPR) dan kod sumber menjadi hak milik Jabatan; c) Memasukkan klausa ke dalam kontrak yang membenarkan jabatan melaksanakan semakan terhadap kod sumber; dan d) Memasukkan klausa ke dalam kontrak yang membenarkan Jabatan mendapat hak pemilikan kod sumber dan melaksanakan pengolohan risiko. 	Pengurus ICT, Pentadbir Sistem dan Pembekal
10.2.8	Ujian Keselamatan Sistem	
	Aktiviti pengujian penerimaan sistem hendaklah dilaksanakan ke atas sistem baru, naik taraf dan versi baru berdasarkan kriteria yang telah ditetapkan.	Pengurus ICT dan Pentadbir Sistem

Bil.	Perkara	Tanggungjawab
	Bagi memastikan integriti data, pengujian hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (<i>input</i>), peringkat pemprosesan data (<i>process</i>) dan peringkat penjanaan laporan (<i>output</i>)	
10.3 Data Ujian		
	Memastikan data yang digunakan untuk pengujian adalah dilindungi.	
10.3.1	Perlindungan Data Ujian	
	Data ujian hendaklah bersesuaian, dilindungi dan dikawal.	Pengurus ICT

BAB 11: HUBUNGAN DENGAN PEMBEKAL

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

Bil.	Perkara	Tanggungjawab
11.1 Keselamatan Maklumat Dalam Hubungan Pembekal		
11.1.1	Polisi Keselamatan Maklumat Ke Atas Pembekal	
	<p>Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a) Pembekal hendaklah menandatangani Surat Akuan Pematuhan PKS Jabatan;</p> <p>b) Pembekal hendaklah menjalani ujian tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); dan</p> <p>c) Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas.</p>	ICTSO/ Pembekal
11.1.2	Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal	
	Perjanjian dengan pihak pembekal hendaklah merangkumi keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan perkhidmatan teknologi maklumat dan komunikasi.	CIO, Pengurus ICT, dan Pembekal
11.1.3	Kawalan Keselamatan Maklumat Dengan Pembekal Dan Pihak Ketiga	
	Perjanjian dengan pembekal hendaklah meliputi risiko keselamatan yang merangkumi perkhidmatan ICT dan kesinambungan bekalan produk dengan pihak ketiga.	ICTSO, Pengurus ICT, Pembekal
11.2 Pengurusan Penyampaian Perkhidmatan Pembekal		
11.2.1	Pemantauan dan Penilaian Perkhidmatan Pembekal	
	Jabatan hendaklah memantau, menyemak dan mengaudit perkhidmatan pembekal secara berkala.	Pentadbir Sistem

Bil.	Perkara	Tanggungjawab
11.2.2	Pengurusan Perubahan Perkhidmatan Pembekal	
	<p>Setiap perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut SOP yang ditetapkan.</p> <p>Perkara-perkara yang perlu diambil kira adalah seperti berikut:</p> <ul style="list-style-type: none"> a) Perubahan di dalam perjanjian bersama pembekal; b) Perubahan yang dilakukan oleh Jabatan bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor. 	Pengurus ICT

BAB 12: PENGURUSAN INSIDEN KESELAMATAN SIBER

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

Bil.	Perkara	Tanggungjawab
12.1 Pengurusan Insiden Dan Penambahbaikan Keselamatan Maklumat		
12.1.1	Tanggungjawab Dan Prosedur	
	Prosedur bagi mengurus insiden keselamatan siber perlu diwujudkan dan didokumenkan. Jabatan bertanggungjawab dalam pengurusan pengendalian insiden keselamatan siber.	Pasukan CSIRT
12.1.2	Pelaporan Insiden Keselamatan Maklumat	
	<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> a) Semua insiden keselamatan siber yang berlaku mesti dilaporkan kepada Pasukan CSIRT. Semua maklumat adalah SULIT dan tidak boleh didedahkan tanpa kebenaran daripada ICTSO; b) Mematuhi prosedur operasi standard (SOP) keselamatan siber Jabatan; 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 CSIRT / National CERT
12.1.3	Pelaporan Kelemahan Keselamatan Maklumat	
	<p>Insiden keselamatan siber adalah meliputi perkara-perkara berikut:</p> <ul style="list-style-type: none"> a) Pelanggaran Polisi (<i>Violation of Policy</i>) Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar PKS. 	Pasukan CSIRT/ National CERT

Bil.	Perkara	Tanggungjawab
	<p>b) Penghalangan Penyampaian Perkhidmatan (<i>Denial of Service</i>)</p> <p>Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal. Termasuk <i>denial of service</i> (DoS), <i>distributed denial of service</i> (DDoS) dan <i>sabotage</i>.</p> <p>c) Pencerobohan (<i>Intrusion</i>)</p> <p>Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (<i>system tampering</i>), pindaan data (<i>modification of data</i>) dan pindaan kepada konfigurasi sistem.</p> <p>d) Pemalsuan (<i>Forgery</i>)</p> <p>Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (<i>information theft/espionage</i>) dan penipuan (<i>hoaxes</i>).</p> <p>e) <i>Spam</i></p> <p>Spam adalah emel yang dihantar ke akaun emel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang-kali (kandungan emel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.</p> <p>f) <i>Malicious Code</i></p> <p>Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia</p>	

Bil.	Perkara	Tanggungjawab
	<p>melibatkan serangan virus, <i>trojan horse</i>, <i>worm</i>, <i>spyware</i> dan sebagainya.</p> <p>g) <i>Harrassment/Threats</i> Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.</p> <p>h) <i>Attempts/Hack Threats/Information Gathering</i> Percubaaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran. Termasuk <i>spoofing</i>, <i>phishing</i>, <i>probing</i>, <i>war driving</i> dan <i>scanning</i>.</p> <p>i) <i>Kehilangan Fizikal (Physical Loss)</i> Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.</p>	
12.1.4	Penilaian Dan Keputusan Insiden Keselamatan Maklumat	
	<p>Agensi hendaklah menilai sama ada serangan diklasifikasikan sebagai insiden.</p> <p>Menentukan Keutamaan Tindakan Ke Atas Insiden Tindakan ke atas insiden yang dilaporkan akan dibuat berasaskan tahap kritikal sesuatu insiden. Keutamaan akan ditentukan seperti berikut:</p> <p>a) <u>Keutamaan 1:</u> Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara.</p> <p>b) <u>Keutamaan 2:</u></p> <ol style="list-style-type: none"> i. Pencerobohan atau percubaan menceroboh melalui infrastruktur Internet ke atas peralatan rangkaian; ii. Penyebaran penafian penyampaian perkhidmatan (<i>distributed denial of service</i>); 	

Bil.	Perkara	Tanggungjawab
	iii. Serangan atau pendedahan keterdedahan terbaru (<i>new vulnerabilities</i>); atau iv. Lain-lain insiden seperti: <ul style="list-style-type: none"> • Pencerobohan melalui pemalsuan identiti; • Pengubahsuaian laman web, perisian, atau mana-mana komponen sistem tanpa pengetahuan, arahan atau persetujuan pihak yang berkenaan; dan • Gangguan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran. 	
12.2 Pelantikan Pegawai Bertanggungjawab		
	Pegawai Keselamatan ICT (ICTSO) dan anggota Pasukan CSIRT hendaklah dilantik secara rasmi dan dimaklumkan kepada warga Jabatan. Insiden keselamatan siber yang melibatkan Maklumat Rahsia Rasmi hendaklah dirujuk kepada CGSO untuk tindakan selanjutnya.	KP / CIO
12.3 Pengumpulan Dan Pengendalian Bukti		
	Maklumat mengenai insiden keselamatan ICT perlu dikumpul, dianalisis dan disimpan bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan. Pasukan CSIRT hendaklah memastikan bahan bukti berkaitan insiden keselamatan siber dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan bukti seperti jejak audit, <i>backup</i> berkala dan <i>off-site backup</i> hendaklah mengikut tatacara pengendalian yang berkuat kuasa. a) Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pengurus ICT

Bil.	Perkara	Tanggungjawab
	<ul style="list-style-type: none"> i. Melindungi integriti bahan bukti; ii. Mengumpul dan menyimpan bahan bukti bagi tujuan analisis; iii. Merekodkan semua maklumat insiden termasuk maklumat pegawai yang terlibat, perisian, perkakasan dan peralatan yang digunakan; iv. Memaklumkan kepada pihak berkuasa perundangan, seperti pegawai undang-undang dan polis (jika perlu); v. Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang diperlukan (jika perlu); dan vi. Menyediakan laporan insiden kepada CIO. 	

BAB 13: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (PKP) (*BUSINESS CONTINUITY MANAGEMENT (BCM)*)

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

Bil.	Perkara	Tanggungjawab
13.1 Kesenambungan Perkhidmatan		
	KP bertanggungjawab memastikan perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan	KP
13.2 Pelan Kesenambungan Perkhidmatan (<i>Business Continuity Plan (BCP)</i>)		
	<p>CIO hendaklah membangunkan Pelan Kesenambungan Perkhidmatan untuk mengekalkan kesinambungan perkhidmatan bagi memastikan tiada gangguan di dalam penyediaan perkhidmatan jabatan. Pelan ini mestilah diperakui oleh pengurusan jabatan dan perkara-perkara berikut perlu diberi perhatian:</p> <ul style="list-style-type: none"> 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 mengemas kini pelan sekurang-kurangnya setahun sekali; f) Membuat <i>backup</i>; dan g) Mewujudkan Pusat Pemulihan Bencana di lokasi lain. 	<p>CIO, Pengurus ICT, ICTSO Pentadbir Sistem ICT, Pemilik Sistem</p>
13.3 Perubahan atau Pengecualian PKP		
	Sekiranya terdapat perubahan/pengemaskinian atau pengecualian yang perlu dilakukan, permintaan secara	<p>CIO, Pengurus ICT, ICTSO</p>

	bertulis termasuk keterangan dan kebenaran untuk pengecualian/perubahan hendaklah dikemukakan kepada KP.	Pentadbir Sistem ICT, Pemilik Sistem
13.4 Program Latihan dan Kesedaran Terhadap PKP		
	Semua kakitangan perlu mempunyai kesedaran dan mengetahui peranan masing-masing terhadap PKP. PB bertanggungjawab dalam memastikan latihan dan program kesedaran terhadap PKP dilaksanakan setiap tahun.	PB
13.5 Pengujian PKP		
	<p>CIO perlu memastikan perkara-perkara berikut:</p> <p>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;</p> <p>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;</p> <p>c) Ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan;</p> <p>d) Jabatan/Bahagian hendaklah memastikan salinan Pelan Kesenambungan Perkhidmatan sentiasa dikemaskini dan dilindungi seperti di lokasi utama; dan</p> <p>e) Komponen PKP seperti Pelan Pemulihan Bencana (<i>Disaster Recovery Plan – DRP</i>), Pelan Komunikasi Krisis (<i>Crisis Communication Plan – CCP</i>) dan Pelan Tindak Balas Kecemasan (<i>Emergency Response Plan – ERP</i>) perlu diuji dua (2) tahun sekali atau selepas perubahan utama, atau yang mana terdahulu.</p>	CIO, Pengurus ICT, ICTSO Pentadbir Sistem ICT, Pemilik Sistem

13.6 Ketersediaan Kemudahan Pemrosesan Maklumat

	Semua sistem aplikasi dan perkakasan yang kritikal hendaklah mempunyai kemudahan <i>redundancy</i> dan diuji (<i>failover test</i>) keberkesanannya mengikut keperluan.	Pentadbir Sistem ICT, Pengurusan ICT dan ICTSO
--	---	--

BAB 14: PEMATUHAN

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

Bil.	Perkara	Tanggungjawab
14.1 Pematuhan Polisi		
	<p>Adalah menjadi tanggungjawab Pengarah Bahagian untuk memastikan bahawa pematuhan dan sebarang pelanggaran dielakkan.</p> <p>Langkah-langkah perlu bagi mengelakkan sebarang pelanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi PKS Jabatan dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.</p>	SEMUA
14.2 Keperluan Perundangan		
	<p>Kakitangan Jabatan perlu memastikan perundangan dan peraturan yang berkuat kuasa dari semasa ke semasa hendaklah dipatuhi.</p>	SEMUA
14.3 Perlindungan dan Privasi Data Peribadi		
	<p>Kakitangan perlu sedar bahawa data kegunaan peribadi yang dijana dalam aset ICT adalah milik jabatan. Pihak pengurusan tidak menjamin kerahsiaan data peribadi yang disimpan dalam aset ICT.</p> <p>Untuk tujuan keselamatan dan penyelenggaraan rangkaian, pegawai yang diberi kuasa perlu mengawasi peralatan, sistem dan rangkaian. Pihak pengurusan berhak mengaudit rangkaian dan sistem secara berkala bagi memastikan ia mematuhi PKS.</p> <p>Pihak pengurusan perlu menggalakkan dasar privasi yang adil dan bertanggungjawab bagi memastikan semua maklumat peribadi digunakan berdasarkan keperluan untuk mengelakkan penyalahgunaan maklumat.</p>	SEMUA

Bil.	Perkara	Tanggungjawab
	<p>Pendedahan maklumat peribadi tentang kakitangan jabatan kepada pihak ketiga tidak sepatutnya berlaku kecuali:</p> <ul style="list-style-type: none"> a) Dikehendaki oleh undang-undang atau peraturan; b) Dengan persetujuan yang jelas dan nyata daripada kakitangan tersebut; atau c) Setelah menerima persetujuan bertulis daripada pihak ketiga di mana maklumat akan dilindungi dengan tahap keselamatan dan privasi yang mengikut undang-undang, peraturan dan kontrak yang berkuat kuasa; dan d) Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pengeluaran yang tidak sah mengikut undang-undang, peraturan, kontrak dan keperluan jabatan. 	
14.4 Semakan Keselamatan Maklumat		
	<p>Semakan keselamatan maklumat mestilah diambil kira seperti berikut:</p> <ul style="list-style-type: none"> a) Pematuhan pemeriksaan ke atas PKS, 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 pengoperasian sistem maklumat bagi meminimalkan ancaman dan meningkatkan ketersediaan sistem; dan c) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. 	<p>Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pemilik Sistem ICT</p>
14.5 Pelanggaran Perundangan		

Bil.	Perkara	Tanggungjawab
	Mengambil tindakan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaiian, kelalaian dan pelanggaran keselamatan termasuk PKS yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972. Antara tindakan yang boleh diambil terhadap pihak ketiga adalah penamatan kontrak.	KP, CIO, Pengurus ICT, ICTSO
14.6 Akuan Pematuhan PKS		
	KP adalah tanggungjawab untuk memastikan setiap pegawai menandatangani Akuan Pematuhan PKS seperti di LAMPIRAN A.	KP, CIO, Pengurus ICT, ICTSO
14.7 Pematuhan Terhadap Hak Harta Intelek (<i>Intellectual Property Rights</i>)		
	Prosedur pengawalan hendaklah dilaksanakan bagi memastikan pematuhan kepada perundangan, peraturan dan keperluan kontrak berkaitan produk yang mempunyai IPR termasuk perisian proprietary.	Pentadbir Sistem ICT, Pemilik Sistem ICT

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 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022
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 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;
8. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
9. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
10. Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan;
11. Akta Tandatangan Digital 1997;
12. Akta Rahsia Rasmi 1972;
13. Akta Jenayah Komputer 1997;
14. Akta Hak Cipta (Pindaan) Tahun 1997;
15. Akta Komunikasi dan Multimedia 1998;
16. Perintah - Perintah Am;
17. Arahan Perbendaharaan;
18. Arahan Teknologi Maklumat 2007;

19. Garis Panduan Keselamatan MAMPU 2004;
20. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
21. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesyinambungan Perkhidmatan
22. Arahan Teknologi Maklumat dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007)
23. Pekeliling Am Bil. 1 Tahun 2009 – Manual Pengurusan Aset Menyeluruh Kerajaan
24. Surat Pekeliling Am Bilangan 1 Tahun 2009 Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan
25. 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)
26. Surat Arahan Ketua Pengarah MAMPU – Amalan Terbaik Penggunaan Media Jaringan Sosial (Tarikh : 8 April 2011)
27. Surat Arahan Ketua Pengarah MAMPU – Pemantapan Penggunaan Dan Pengurusan E-Mel. (Tarikh : 1 Julai 2010)
28. Surat Arahan Ketua Pengarah MAMPU – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam. (5 Mac 2010)
29. Surat Arahan Ketua Pengarah MAMPU – Garis Panduan Transisi Protokol Internet Versi 6 (IPv6) Sektor Awam. (Tarikh : 4 Januari 2010)
30. Surat Arahan Ketua Pengarah MAMPU – Penggunaan Media Jaringan Sosial Di Sektor Awam. (Tarikh : 19 November 2009)
31. Surat Arahan Ketua Pengarah MAMPU – Penggunaan Smartphone, Personal Digital Assistant Dan Alat Komunikasi Mudah Alih Sebagai Saluran Komunikasi Tambahan (Tarikh : 15 September 2009)
32. Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam (Ogos 2010)
33. Arahan Teknologi Maklumat Dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007)
34. Garis Panduan IT Outsourcing (Oktober 2006)
35. Garis Panduan Penyimpanan dan Pemeliharaan Rekod Elektronik Sektor Awam
36. Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara

37. Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara.
38. Pekeliling Am Bil. 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam.
39. Rancangan Malaysia ke-11.
40. Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam.
41. Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam 25 Januari 2015.
42. Dasar Kriptografi Negara 12 Julai 2013
43. Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology* ICT Kerajaan SPP 3/2013.
44. Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan.
45. Garis Panduan Perolehan ICT Kerajaan Jabatan Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013.
46. Arahan Ketua Pegawai Keselamatan Kerajaan 5 jun 2012 – Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam
47. PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua).
48. Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 Nov 2010.
49. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesenambungan Perkhidmatan Agensi Sektor Awam, 22 Jan 2010.
50. Akta 709 – Akta Perlindungan Data Peribadi 2010.
51. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan, 23 Nov 2007.
52. 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
53. 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.
54. Akta 658 – Akta Perdagangan Elektronik 2006.
55. Akta 629 – Akta Arkib Negara 2003.
56. Akta 606 – Akta Cakera Optik 2000.
57. Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987).

58. Akta 298 – Kawasan Larangan Tempat Larangan 1959
59. Akta 56 – Akta Keterangan 1950.
60. National Cyber Security Policy (NCSP)
61. Guideline to Determine Information Security Professionals Requirement for the CNII Agencies /Organisations.
62. Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara.
63. Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi.
64. Perintah Am Bab D.
65. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA) versi 1.0 April 2016



**AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
JABATAN WILAYAH PERSEKUTUAN**

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

Tandatangan :

Tarikh :

Pengesahan Pegawai Keselamatan ICT

.....

(Tandatangan & Cop Jawatan)

Jabatan Wilayah Persekutuan

Tarikh:

* PKS boleh dicapai menerusi <http://www.jwp.gov.my>

**PEMBEKAL
LAMPIRAN B (II)**

LAMPIRAN B (II)



**AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
JABATAN WILAYAH PERSEKUTUAN**

Nama (Huruf Besar) :
No. Kad Pengenalan :
Nama Syarikat :
No. Pendaftaran Syarikat :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam PKS; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan :

Tarikh :

Pengesahan Pegawai Keselamatan ICT

.....

(Tandatangan & Cop Jawatan)

Jabatan Wilayah Persekutuan

Tarikh:

* PKS boleh dicapai menerusi <http://www.jwp.gov.my>