PEJABAT PENGARAH TANAH DAN GALIAN
WILAYAH PERSEKUTUAN

POLISI KESELAMATAN SIBER

KANDUNGAN

SEJARAH POLISI KESELAMATAN SIBER PPTGWP

Tarikh	Versi	Kelulusan	Tarikh Kuatkuasa
31 Disember 2022	1.0	JPICT PPTGWP Bil. 1/2023	

PENGENALAN

1. Polisi Keselamatan Siber Pejabat Pengarah Tanah dan Galian Wilayah Persekutuan (PKS PPTGWP) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna di PPTGWP mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT PPTGWP.

OBJEKTIF

2. PKS PPTGWP dibangunkan untuk menjamin kesinambungan urusan PPTGWP dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi PPTGWP. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

   Objektif utama Keselamatan ICT PPTGWP adalah seperti berikut:

   (a) Menerangkan kepada semua pengguna merangkumi warga PPTGWP, pembekal dan pihak berkepentingan yang yang mempunyai urusan dengan perkhidmatan ICT PPTGWP mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber.

   (b) Memastikan kelancaran operasi PPTGWP dan meminimumkan kerosakan atau kemusnahan;

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

   (d) Mencegah salah guna atau kecurian aset ICT Kerajaan.

   (e) Memperkemaskan pengurusan keselamatan ICT PPTGWP.

PERNYATAAN POLISI KESELAMATAN SIBER PPTGWP

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

menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

4. Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

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

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

(b) **Integriti** : Data dan maklumat hendaklah tepat, lengkap dan dikemas kini. 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) **Kebolehsediaan** : Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

7. Selain itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT PPTGWP, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin

timbul dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

8. Polisi Keselamatan Siber PPTGWP terdiri daripada empat belas (14) bidang kawalan keselamatan yang akan diterangkan dengan lebih jelas dan teratur.

SKOP PKS PPTGWP

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

(a) Data dan maklumat termasuk *hardcopy* atau *softcopy* 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.

10. Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, PKS PPTGWP ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, 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 :

(a) **Peralatan ICT**

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan PPTGWP. Contoh : komputer, pelayan, peralatan komunikasi dan sebagainya.

(b) **Perisian**

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang

disimpan dalam sistem ICT. Contoh seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada PPTGWP.

(c) **Perkhidmatan**

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

i) Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;

ii) Sistem halangan akses seperti sistem kad akses; dan

iii) Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin,sistem pencegah kebakaran dan lain-lain.

(d) **Data atau Maklumat**

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif PPTGWP. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod PPTGWP, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

(e) **Manusia**

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

(f) **Premis Komputer dan Komunikasi**

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara **(a)** - **(e)** di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

PRINSIP KESELAMATAN

11. Prinsip-prinsip yang menjadi asas kepada PKS PPTGWP dan perlu dipatuhi adalah seperti berikut :

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

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

(b) **Hak akses minimum**

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna / bidang tugas;

(c) **Akauntabiliti**

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap *sensitiviti* sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat bolehdipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa

iii) Menentukan maklumat sedia untuk digunakan;

iv) Menjaga kerahsiaan kata laluan;

v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

vi) Memberi perhatian kepada maklumat berperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

(d) **Pengasingan**

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

(e) **Pengauditan**

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

(f) **Pematuhan**

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

(g) **Pemulihan**

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

(h) **Saling Bergantungan**

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

PENILAIAN RISIKO KESELAMATAN ICT

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

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

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

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

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

(b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan

oleh pengurusan agensi;

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

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

PEJABAT PENGARAH TANAH DAN GALIAN
WILAYAH PERSEKUTUAN

BAHAGIAN 01

POLISI KESELAMATAN MAKLUMAT

BAHAGIAN 01	POLISI KESELAMATAN MAKLUMAT

Objektif

Menerangkan dan memastikan hala tuju pengurusan terhadap keselamatan maklumat adalah selaras dengan keperluan perkhidmatan PPTGWP dan peraturan serta perundangan berkaitan yang sedang berkuatkuasa.

Perkara	Peranan
B01/01 Pelaksanaan Polisi	
PKS ini dilaksanakan oleh Pengarah Tanah dan Galian (PTG) dengan dibantu oleh Jawatankuasa Pemandu ICT PPTGWP yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pengurus ICT, Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.	PTG
B01/02 Penyebaran Polisi	
PKS ini perlu disebarkan kepada semua yang terlibat dengan infrastruktur ICT PPTGWP termasuk warga PPTGWP, pembekal, pakar runding dan lain-lain.	ICTSO
B01/03 Pemakaian Polisi	
PKS ini terpakai kepada semua warga PPTGWP dan juga Pihak Ketiga yang berurusan dengan PPTGWP.	Pengguna / Pihak Ketiga
B01/04 Penyelenggaraan Polisi	
Polisi ini tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Prosedur semakan semula polisi ini adalah seperti berikut: (a) Menyemak sekurang-kurangnya satu (1) kali setahun atau mengikut keperluan semasa bagi mengenal pasti dan menentukan perubahan yang diperlukan; (b) Mengemukakan cadangan pindaan atau perubahan secara bertulis, membuat pembentangan dan mendapatkan kelulusan	ICTSO

Perkara	Peranan
pindaan daripada Jawatankuasa Pemandu ICT (JPICT) PPTGWP; dan (c) Memaklumkan pindaan atau perubahan polisi yang telah dipersetujui kepada semua pengguna.	

BAHAGIAN 02
ORGANISASI KESELAMATAN MAKLUMAT

BAHAGIAN 02	ORGANISASI KESELAMATAN MAKLUMAT

Objektif

Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber (PKS) PPTGWP.

Perkara	Peranan
B02/01 Infrastruktur Organisasi Keselamatan	
B02/01/01 Pengarah Tanah dan Galian (PTG)	
Peranan dan tanggungjawab PTG adalah seperti berikut: (a) memastikan semua pengguna memahami peruntukan-peruntukan di bawah Polisi Keselamatan Siber (PKS) PPTGWP; (b) memastikan semua pengguna mematuhi PKS PPTGWP; (c) memastikan semua keperluan PPTGWP seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan adalah mencukupi; dan (d) Memastikan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam PKS PPTGWP.	PTG
B02/01/02 Ketua Pegawai Digital (CDO)	
Ketua Pegawai Digital (CDO) PPTGWP ialah Timbalan Pengarah, Sektor Khidmat Pengurusan. Peranan dan tanggungjawab CDO adalah seperti berikut: (a) meneraju inisiatif pendigitalan di kementerian/agensi melalui penggunaan data, analitis dan teknologi digital; (b) mewujudkan budaya berpacukan data dalam sektor awam yang mengamalkan pendekatan *principal-based* melalui penggunaan data dan teknologi digital;	CDO

Perkara	Peranan
(c) mentransformasikan penyampaian perkhidmatan digital di PPTGWP berfokuskan pengalaman pelanggan (*customer experience*) yang berteraskan konsep *Whole-of-Government* melalui inovasi melibatkan perkongsian data, data terbuka dan teknologi baru muncul; (d) menilai, menyelaras, memperaku keperluan perkhidmatan digital, *Technical Service Design* dan bajet pembangunan serta mengurus agensi sebagai pelaksana inisiatif dan projek pendigitalan; (e) meneraju perubahan melalui Penjajaran Pelan Strategik Pendigitalan (PSP) PPTGWP selari dengan; (i) memastikan PSP PPTGWP selari dengan PSP Sektor Awam, Pelan Pengurusan Risiko dan Pelan Pengurusan Perubahan; (ii) memastikan blueprint Enterprise Architecture (EA) agensi tersedia; dan (iii) memantapkan struktur tadbir urus pendigitalan agensi dan menyelaras penggunaan dasar, standard dan amalan terbaik global. (f) Melaporkan pelaksanaan dan kemajuan transformasi pendigitalan PPTGWP.	
B02/01/03 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) PPTGWP ialah Timbalan Pengarah, Sektor Khidmat Pengurusan. Peranan dan tanggungjawab CIO adalah seperti berikut: (a) Membantu Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan keselamatan ICT; (c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan Polisi Keselamatan Siber PPTGWP PPTGWP serta pengurusan risiko dan pengauditan; dan	CIO

Perkara	Peranan
(d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT PPTGWP.	
B02/01/04 Pegawai Keselamatan Maklumat (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) yang dilantik berperanan dan bertanggungjawab seperti berikut: (a) Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan organisasi; (b) Mengurus keseluruhan program keselamatan ICT PPTGWP; (c) Menguatkuasakan pelaksanaan PKS PPTGWP di semua cawangan/sektor/bahagian di PPTGWP; (d) Memberi penerangan dan pendedahan berkenaan PKS PPTGWP kepada semua pengguna; (e) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS PPTGWP; (f) Menjalankan tugas pengurusan risiko; (g) Menjalankan audit, kajian semula, merumus tindak balas pengurusan PPTGWP berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (h) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (i) Melaporkan insiden keselamatan ICT kepada Agensi Keselamatan Siber Negara (NACSA) dan memaklumkan kepada CIO; (j) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;	ICTSO

Perkara	Peranan
(k) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; (l) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan (m) Koordinator Pelan Pengurusan Pemulihan Bencana (DR Koordinator) PPTGWP.	
B02/01/05 Pengurus ICT	
Pengurus ICT disandang oleh Ketua Penolong Pengarah Bahagian Pengurusan Maklumat (BPM) PPTG WPKL, Pegawai Teknologi Maklumat PPTG WP Putrajaya dan Penolong Pegawai Teknologi Maklumat PPTG WP Labuan. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Memastikan PKS PPTGWP dilaksanakan dan dipatuhi di bahagian; (b) Memastikan semua pengguna di PPTGWP mematuhi dasar, piawaian dan garis panduan keselamatan ICT, dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT; (c) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan PPTGWP; (d) Menentukan kawalan hak akses semua pengguna ICT terhadap aset ICT PPTGWP dan membuat semakan berkala; (e) Merangka dan menyemak pelan kontingensi ICT PPTGWP; (f) Melaporkan sebarang masalah berkaitan keselamatan ICT kepada CIO; dan (g) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT PPTGWP.	Pengurus ICT

Perkara	Peranan
B02/01/06 Pentadbir ICT	
Pentadbir ICT terdiri daripada seperti berikut: (i) Pentadbir Rangkaian dan Keselamatan; (ii) Pentadbir Sistem Aplikasi; (iii) Pentadbir Pusat Data; (iv) Pentadbir Portal (Web Master); (v) Pentadbir E-mel; dan (vi) Pentadbir Media Sosial.	Pentadbir Sistem
B02/01/06/01 Pentadbir Rangkaian Dan Keselamatan	
Peranan dan tanggungjawab Pentadbir Rangkaian dan Keselamatan adalah seperti berikut: (a) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di PPTGWP beroperasi sepanjang masa; (b) Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; (c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; (d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; (e) Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT; (f) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian PPTGWP secara tidak sah seperti melalui peralatan modem dan dial-up; (g) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; (h) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; dan (i) Memastikan maklumat perhubungan perlu dikemas	Pentadbir Rangkaian dan Keselamatan

Perkara	Peranan
kini dari semasa ke semasa.	
B02/02/06/02 Pentadbir Sistem Aplikasi	
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: (a) Mengkaji cadangan pembangunan atau penyelarasan sistem atau modul di PPTGWP; (b) Membuat kajian semula serta memperbaiki sistem atau modul sistem sedia ada di PPTGWP; (c) Membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem atau modul di PPTGWP; (d) Membuat pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa; (e) Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem atau modul; (f) Menyediakan dokumentasi sistem atau modul dan manual pengguna; (g) Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; (h) Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; (i) Memastikan *virus pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi terkemas kini.	Pentadbir Sistem Aplikasi
B02/01/06/03 Pentadbir Pusat Data	
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: (a) Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; (b) Memastikan keselamatan data dan sistem aplikasi	Pentadbir Pusat Data

Perkara	Peranan
yang berada dalam Pusat Data; (c) Menjadualkan dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala; (d) Menyediakan perancangan Pelan Pemulihan Bencana (DRP) bagi memasti kesinambunagn perkhidmatan; (e) Melaksanakan prinsip-prinsip PKS; (f) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan; (g) Melaporkan sebarang pelanggaran keselamatan Pusat Data PPTGWP kepada ICTSO; dan (h) Memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.	
B02/01/06/04 Pentadbir Portal (Webmaster)	
Peranan dan tanggungjawab Pentadbir Portal adalah seperti berikut: (a) Menerima kandungan laman web yang telah disahkan kesahihandan terkini daripada sumber yang sah; (b) Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; (c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam,menceroboh dan mengubahsuai muka laman; (d) Menghadkan capaian Pentadbir Laman Web bahagian/unit ke web server; (e) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; (f) Melaporkan sebarang pelanggaran keselamatan laman portal kepada CERT PPTGWP.	Pentadbir Portal (Webmaster)

Perkara	Peranan
B02/01/06/05 Pentadbir E-Mel	
Peranan dan tanggungjawab pentadbir E-Mel adalah seperti berikut: (a) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Pengurus ICT. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar polisi dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; (b) Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; (c) Memastikan pengguna e-mel PPTGWP berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel PPTGWP dan pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan; (d) Memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi; (e) Mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi; dan (f) Memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.	Pentadbir E-Mel
B02/01/06/06 Pentadbir Media Sosial PPTGWP	
Peranan dan tanggungjawab Pentadbir Media Sosial PPTGWP adalah seperti berikut: (a) Maklumkan kepada semua ahli kumpulan, sebab utama kumpulan aplikasi pesanan diwujudkan dan memikirkan sama ada peraturan asas diperlukan; (b) Prihatin terhadap peraturan atau syarat-syarat yang digariskan oleh penyedia platform; (c) Sentiasa semak *posting* atau komen (dengan	Pentadbir Media Sosial

Perkara	Peranan
seorang *moderator*, jika boleh) (d) Menegur *posting* atau komen untuk memastikan perbincangan berada di landasan yang betul; (e) Mempertimbangkan untuk mengeluarkan atau menyekat mereka yang terus membuat *posting* atau komen jelik; dan (f) Melaporkan sebarang pelanggaran polisi penggunaan yang sedang berkuat kuasa.	
B02/01/07 Pegawai Aset	
Pegawai Aset ICT ialah pegawai yang dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab Pegawai Aset ICT adalah seperti berikut: (a) Memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan; (b) Memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan/ Bahagian; (c) Memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset; (d) Memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua Jabatan/ Pegawai Aset/ Pegawai pegawai lain yang diberi kuasa oleh Ketua Jabatan; (e) Memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/penggantian/naik-taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira; (f) Memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama PPTGWP/Bahagian	Pegawai Aset

Perkara	Peranan
berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan; (g) Memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan; (h) Memastikan senarai daftar induk aset ICT Kerajaan disediakan; (i) Memastikan senarai aset ICT Kerajaan disediakan mengikut lokasi dan format Senarai Aset ICT Kerajaan dalam dua (2) buah salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset ICT/ Pembantu Pegawai Aset ICT dan satu (1) salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi; (j) Memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan; (k) Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan; (l) Merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya satu (1) kali setahun; dan (m) Memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.	
B02/01/08 Pengguna	
Pengguna terdiri daripada warga PPTGWP dan pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan. Peranan dan tanggungjawab pengguna adalah seperti berikut: (a) Pengguna perlu membaca, memahami dan mematuhi PKS PPTGWP; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;	Pengguna

Perkara	Peranan
(c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; (d) Melaksanakan prinsip-prinsip PKS dan menjaga kerahsiaan maklumat PPTGWP; (e) Mengawal aktiviti penggunaan media sosial seperti di bawah: i) Mengelak ketirisan maklumat; ii) Tidak memberi atau mendedahkan sebarang komen atau pernyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan; iii) Tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasi sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan iv) Tidak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja. (f) Melaporkan aktiviti yang tidak normal berkaitan ICT kepada ICTSO atau Pegawai ICT PPTGWP; dan (g) Menandatangani Akuan Pematuhan Polisi Keselamatan Siber PPTGWP seperti di **Lampiran B**.	
B02/01/09 Pihak Ketiga	
Peranan dan tanggungjawab Pihak Ketiga adalah seperti berikut : (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;	Pihak Ketiga

Perkara	Peranan
(c) Menjaga kerahsiaan maklumat berkaitan penggunaan ICT; (d) Menandatangani perakuan pematuhan keselamatan siber yang ditetapkan oleh Kerajaan Malaysia atau peraturan yang setara/berkaitan yang berkuat kuasa; (e) Melaporkan aktiviti yang tidak normal berkaitan ICT kepada ICTSO / Pegawai ICT PPTGWP; dan (f) Mendapatkan kelulusan untuk menggunakan kemudahan, perkhidmatan dan peralatan ICT PPTGWP.	
B02/01/10 Pasukan Tindak Balas Insiden Keselamatan Siber PPTGWP	
Keanggotaan Pasukan Tindak Balas Insiden Keselamatan Siber (*Cyber Security Incident Response Team* - CSIRT) PPTGWP adalah seperti berikut: Pengarah CSIRT : Timbalan Pengarah, Sektor Khidmat Pengurusan, PPTGWP KL Pengurus CSIRT : Ketua Penolong Pengarah, BPM PPTGWP KL Ahli CSIRT : ▪ Pegawai Teknologi Maklumat PPTGWP ▪ Penolong Pegawai Teknologi Maklumat PPTGWP * Tertakhluk kepada pelantikan. Peranan dan tanggungjawab CSIRT PPTGWP adalah; (a) Memantau, mengesan insiden, menerima dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti insiden serta menilai impak keselamatan siber;	CSIRT PPTGWP

Perkara	Peranan
(b) Merekodkan dan menjalankan siasatan awal insiden yang diterima; (c) Melaksanakan pengurusan dan pengendalian insinden keselamatan siber serta mengambil tindakan awal pemulihan; (d) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan; (e) Melaporkan insiden keselamatan siber kepada agensi yang menyelianya (sekiranya ada) dan NC4; (f) Menasihati agensi di bawah PPTGWP mengambil tindakan pemulihan dan pengukuhan; (g) Menyebarkan makluman/amaran berkaitan insiden kepada agensi lain di bawah seliaanya (sekiranya ada); dan (h) Memastikan fail log disimpan sekurang-kurangnya enam (6) bulan di tempat selamat.	
B02/01/11 Jawatankuasa Pemandu ICT (JPICT) PPTGWP	
Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa yang bertanggungjawab dalam menyelaras dan memantau pelaksanaan projek ICT serta membincangkan perkara berkaitan keselamatan ICT. Keanggotaan Jawatankuasa Pemancu ICT (JPICT) PPTGWP adalah seperti berikut: Pengerusi : Pengarah Tanah dan Galian	JPICT PPTGWP

Perkara	Peranan
Ahli-ahli : ▪ Timbalan Pengarah PPTGWP ▪ Semua Ketua Bahagian/Unit ▪ Pegawai Teknologi Maklumat ▪ Pegawai Undang-Undang ▪ Ketua Unit Komunikasi Korporat ▪ Ketua Unit Integriti ▪ Ahli-ahli jemputan berkaitan (mengikut keperluan) Urus setia : Bahagian Pengurusan Maklumat, PPTG WPKL Peranan dan tanggungjawab JPICT PPTGWP adalah : (a) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT agensi; (b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT agensi; (c) Merancang dan menyelaras pembangunan dan pelaksanaan program/projek ICT agensi; (d) Menyelaras dan menyeragamkan pembangunan ICT agensi agar selari dengan pelan strategik organisasi dan pelan strategik ICT agensi; (e) Meluluskan projek ICT agensi berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan; (f) Mengikuti dan memantau perkembangan program ICT agensi serta memahami keperluan, masalah dan isu yang dihadapi dalam pembangunan dan pelaksanaan ICT; (g) Merancang dan menentukan langkah-langkah keselamatan ICT;	

Perkara	Peranan
(h) Mengemukakan perolehan ICT yang telah diluluskan di peringkat JPICT Agensi kepada Kementerian/ JTISA untuk kelulusan (jika berkaitan); dan (i) Mengemukakan laporan kemajuan projek ICT yang telah diluluskan kepada Kementerian dan JTISA (jika berkaitan) mengikut tempoh yang telah ditetapkan.	
B02/02 Peranti Mobil dan Telekerja (Teleworking)	
a) Peranti Mudah Alih Milik Persendirian 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) Telekerja (Teleworking) 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.	Pengguna

BAHAGIAN 03

KESELAMATAN SUMBER MANUSIA

BAHAGIAN 03	KESELAMATAN SUMBER MANUSIA

Objektif

Memastikan semua pengguna yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklahmematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

Perkara	Peranan
B03/01 Sebelum Perkhidmatan	
Memastikan semua pengguna yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: a) menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua pengguna yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan; b) lulus tapisan keselamatan dan menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber untuk semua pengguna PPTGWP; c) memastikan pihak luaran menandatangani Akuan Pematuhan PKS PPTGWP (**Lampiran B**), Akuan Berkanun PPTGWP (**Lampiran C**) dan lulus Tapisan Keselamatan dan; d) mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengurus ICT
B03/02 Semasa Perkhidmatan	
Memastikan semua pengguna yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong	Pengurus ICT

Perkara	Peranan
PKS PPTGWP dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi termasuk yang berikut: a) memastikan semua pengguna yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan PPTGWP; b) memastikan latihan dan program kesedaran yang berkaitan keselamatan ICT diberikan kepada pengguna dari semasa ke semasa; c) memastikan prosedur latihan jabatan sentiasa dikemas kini bersesuaian dengan fungsi tugas semasa setiap pengguna; d) memastikan adanya tindakan tatatertib/ atau perundangan ke atas semua pengguna sekiranya berlaku pelanggaran keselamatan maklumat jabatan; dan e) memantapkan pengetahuan berkaitan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	
B03/03 Bertukar Atau Tamat Perkhidmatan	
Memastikan pertukaran atau tamat perkhidmatan semua pengguna yang berkepentingan diuruskan dengan teratur. Perkara yang perlu dipatuhi termasuk: a) memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan PPTGWP dan/atau terma perkhidmatan.	Pengurus ICT

BAHAGIAN 04
PENGURUSAN ASET

BAHAGIAN 04	PENGURUSAN ASET

Objektif

Memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT PPTGWP.

Perkara	Peranan
B04/01 Akauntabiliti Aset ICT	
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT PPTGWP. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: a) memastikan semua aset ICT dikenal pasti, dikelaskan, didokumenkan, diselenggarakan dan dilupuskan. Maklumat aset direkodkan dan dikemas kini dalam Sistem Pengurusan Aset (SPA), Kad Daftar Harta Modal dan Aset Alih Bernilai Rendah sebagaimana mengikut Pekeliling Perbendaharaan AM 2 Tahun 2018:Tatacara Pengurusan Aset Alih Kerajaan atau senarai aset yang berkaitan; b) memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di PPTGWP. d) memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan; e) setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan f) penggunaan aset ICT PPTGWP mestilah tujuan tugas rasmi sahaja.	Pegawai Aset ICT, Pengguna

Perkara	Peranan
B04/02 Peminjaman Dan Pemulangan Aset ICT	
Peminjaman Langkah-langkah perlu diambil termasuklah seperti berikut: a) mendapatkan kelulusan mengikut peraturan yang telah ditetapkan 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. **Pemulangan** Memastikan semua aset ICT dikembalikan mengikut peraturan dan atau terma perkhidmatan yang ditetapkan bagi pegawai yang : a) bertukar keluar; b) bersara; c) ditamatkan perkhidmatan; dan d) diarahkan oleh Ketua Jabatan Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.	Pegawai Aset ICT
B04/03 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada PPTGWP. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan dan dilabel sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:	Pegawai Pengelas

Perkara	Peranan
a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad	
B04/04 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: a) menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) menentukan maklumat sedia untuk digunakan. menjaga kerahsiaan kata laluan; d) mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; e) melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; f) menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum; dan g) mewujudkan salinan pendua maklumat penting bagi mengurangkan risiko kehilangan dan kemusnahan.	Pengguna
B04/05 Pengelasan Dan Pengendalian Data Terbuka	
Data Terbuka ialah data yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan.	Pengguna

Perkara	Peranan
Jabatan akan menyediakan set data terbuka berdasarkan bidang atau sektor atau kluster. Kategori set data ini tidak terhad dan boleh berubah mengikut fungsi teras dan keperluan semasa Jabatan. Data terbuka yang telah diperakukan oleh Jabatan akan dikemukakan ke JPM untuk kelulusan dan seterusnya diterbitkan ke Portal Data Terbuka Sektor Awam (DTSA) di bawah pengurusan MAMPU.	
B04/06 Pengendalian Media Storan	
Media storan merupakan peralatan yang digunakan untuk menyimpan data dan maklumat seperti *optical disk, flash disk, hard disk, USB flash drive, catridge tape, compact disc* (CD). Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil: a) semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan; b) bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu; c) semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat; d) semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti (data safe) yang mempunyai ciri-ciri keselamatan termasuk tahan daripada dipecahkan, api, air dan medan magnet; e) storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang lebih privasi dan tidak	Pentadbir Sistem, Pegawai Aset ICT

Perkara	Peranan
terbuka kepada umum. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; f) akses dan pergerakan kepada media storan perlu direkodkan; g) perkakasan *backup* hendaklah diletakkan di tempat yang selamat dan terhad kepada pengguna yang dibenarkan sahaja; dan h) sebarang kehilangan media storan yang berlaku hendaklah dilaporkan mengikut Prosedur Pelaporan Insiden.	

BAHAGIAN 05
KAWALAN CAPAIAN

BAHAGIAN 05	KAWALAN CAPAIAN

Objektif

Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT.

Perkara	Peranan
B05/01 Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Pentadbir Sistem
B05/02 Pengurusan Capaian Pengguna	
B05/02/01 Pendaftaran Pengguna	
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah langkah berikut: a) akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b) akaun *user id* hendaklah mencerminkan identiti pengguna; c) pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; d) penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan i) Pentadbir Sistem boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:	Pentadbir Sistem, Pengguna

Perkara	Peranan
ii) pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan; iii) bertukar bidang tugas kerja; iv) bertukar ke agensi lain; v) bersara; atau vi) ditamatkan perkhidmatan.	
B05/02/02 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui *(*need-to-know-basis*)*. Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja.	Pentadbir Sistem
B05/02/03 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh PPTGWP seperti berikut: a) dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan antara huruf, nombor (alphanumerik) dan aksara khas kecuali bagi perkakasan dan perisian yang pengurusan kata laluan yang terhad; c) kekerapan penukaran dan penggunaan kata laluan adalah mengikut ketetapan polisi pengurusan kata laluan yang berkuat kuasa; d) kata laluan sistem pengoperasian (OS) atau *Directory Service* hendaklah diaktifkan terutamanya pada	Pentadbir Sistem Pengguna

Perkara	Peranan
komputer yang terletak di ruang guna sama; e) kata laluan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun; f) kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; h) kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; j) kata laluan hendaklah disimpan dalam bentuk yang telah disulitkan (encripted) ; dan k) sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
B05/03 Capaian Sistem Pengoperasian	
B05/03/01 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian kepada sumber sistem komputer. Kemudahan ini juga perlu bagi: a) mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b) mengenal pasti identiti, terminal atau lokasi bagi	Pentadbir Sistem

Perkara	Peranan
setiap pengguna yang dibenarkan; c) mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; d) merekodkan capaian yang berjaya dan gagal; e) membekalkan kemudahan untuk pengesahan (bagi sistem kata laluan kunci digunakan, kualiti kata kunci perlu mendapat pengesahan); dan f) mengehadkan masa penggunaan rangkaian bagi pengguna. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; b) mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; c) menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan d) menyediakan tempoh penggunaan mengikut kesesuaian. Perkara-perkara yang perlu dipatuhi termasuk berikut: a) mengawal capaian ke atas sistem operasi menggunakan prosedur *log on* yang terjamin; b) mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna; c) mewujudkan fungsi pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah kukuh mengikut polisi kata laluan yang berkuat kuasa;	

Perkara	Peranan
d) menghadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan e) mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
B05/03/02 Token/Sijil Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) penggunaan token Kerajaan Elektronik (Token EG) atau sijil digital hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b) token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c) perkongsian penggunaan token adalah tidak dibenarkan sama sekali; dan d) sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pengeluar token.	Pengguna
B05/04 Capaian Aplikasi Dan Maklumat	
Bertujuan melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di PPTGWP adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: a) pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b) setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi	Pentadbir Sistem, Pegawai Aset ICT

Perkara	Peranan
mengesan aktiviti-aktiviti yang tidak diingini; c) memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d) memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; e) capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; f) maklumat tarikh *login* terakhir hendaklah direkodkan; dan g) digalakkan *session timeout* dilaksanakan.	
B05/05 Capaian Jarak Jauh	
a) Capaian jarak jauh yang dimaksudkan merangkumi: i) capaian daripada sistem rangkaian dalaman; dan ii) capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *telecommuting*. b) Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (encryption); c) Lokasi bagi akses ke sistem ICT PPTGWP hendaklah dipastikan selamat; dan d) Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Rangkaian dan Keselamatan. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Pentadbir Sistem, Pengguna

Perkara	Peranan
B05/06 Kawalan Capaian Rangkaian	
B05/06/01 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan; a) mewujudkan segemen rangkaian yang besesuaian bagi membezakan di anatra rangkaian PPTGWP dan rangkaian awam; b) mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya; c) memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; d) capaian pengguna jarak jauh (remote user) perlulah dikawal dan dipantau; e) capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal; dan f) semua rangkaian yang dikongsi (shared networks), terutama yang keluar daripada rangkaian PPTGWP, polisi perlu diwujudkan untuk mengawal capaian oleh pengguna.	Pentadbir Rangkaian dan Keselamatan
B05/06/02 Capaian Internet	
a) penggunaan Internet di PPTGWP hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian dan Keselamatan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian PPTGWP;	Pentadbir Rangkaian dan Keselamatan

Perkara	Peranan
b) penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;	Pengurus ICT
c) polisi *Content Filtering* mestilah digunakan dan dipantau bagi mengawal akses Internet. Pengguna boleh memohon pengecualian mengikut fungsi kerja untuk pertimbangan;	Pentadbir Rangkaian dan Keselamatan
d) penggunaan proksi yang telah ditetapkan oleh PPTGWP bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi pekeliling semasa yang dikeluarkan; dan	
e) penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan; dan	
f) penggunaan kemudahan Internet peribadi di pejabat seperti modem, *hotspot* dan sebagainya untuk tujuan sambungan ke Internet adalah tidak dibenarkan kecuali mendapat kelulusan CIO/CDO/Pengurus ICT.	
B05/07 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: a) merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kehilangan atau kerosakan; b) peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan; dan c) memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.	Pegawai Aset ICT, Pengguna

Perkara	Peranan
B05/08 *Bring Your Own Device* (BYOD)	
BYOD merupakan peralatan mudah alih persendirian seperti telefon pintar, tablet dan laptop yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian Jabatan. Pengguna yang menggunakan kemudahan wifi jabatan atau *data line* persendirian untuk akses kepada Internet tertakluk kepada PKS PPTGWP. Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah langkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut : a) mengelak risiko kebocoran maklumat rasmi; b) mengelakkan ancaman risiko keselamatan ICT; c) memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi jabatan; dan d) meningkatkan integriti data. Bagi mengawal dan memantau pelaksanaan BYOD, mekanisme kawalan diwujudkan seperti berikut: a) mendaftarkan penggunaan peralatan mudah alih yang digunakan melalui AD; b) mengaktifkan fungsi keselamatan kata laluan bagi mengelakkan akses yang tidak dibenarkan; dan c) melaporkan kehilangan peralatan mudah alih kepada ICTSO. Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.	Pengguna

BAHAGIAN 06
KRIPTOGRAFI

BAHAGIAN 06	KRIPTOGRAFI

Objektif

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

Perkara	Peranan
B06/01 Kriptografi	
Kriptografi bermaksud sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja. Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. Kriptografi merangkumi kaedah-kaedah seperti berikut: a) Kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan dan dibuat enkripsi. b) Penggunaan PKI (Public Key Infrastructure) selamat yang dibekalkan/diiktiraf oleh Kerajaan. c) Penggunaan tandatangan digital digalakkan kepada semua pengguna yang menguruskan maklumat terperingkat secara elektronik; Pengurusan ke atas *Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	Pentadbir Sistem, Pengguna

BAHAGIAN 07

KESELAMATAN FIZIKAL DAN PERSEKITARAN

BAHAGIAN 07	KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif

Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.

Perkara	Peranan
B07/01 Keselamatan Kawasan	
B07/01/01 Kawasan Larangan Lokasi ICT	
Kawasan larangan lokasi ICT bagi PPTGWP ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga PPTGWP yang tertentu sahaja. Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT. Kawasan larangan lokasi ICT PPTGWP adalah Pusat Data PPTGWP. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut: a) sumber data atau *server,* peralatan komunikasi dan storan perlu ditempatkan di pusat data yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran; b) akses adalah terhad kepada warga PPTGWP yang telah diberi kuasa sahaja dan dipantau pada setiap masa; c) pemantauan dibuat menggunakan Sistem CCTV atau peralatan-peralatan lain yang sesuai; d) peralatan keselamatan seperti CCTV dan pengimbas biometrik perlu diperiksa secara berjadual; e) butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;	Pentadbir Pusat Data

Perkara	Peranan
f) pihak luaran yang dibawa masuk mesti diawasi atau diiringi oleh pegawai bertanggungjawab di sepanjang tempoh di lokasi mengikut keperluan sewajarnya; g) lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam; h) memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; i) memperkukuhkan dinding dan siling; j) mengehadkan jalan keluar masuk; dan k) menyediakan tempat taua bilik khas untuk pihak ketiga.	
B07/01/02 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Warga PPTGWP i) semua warga hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; dan ii) semua pas keselamatan hendaklah diserahkan kembali kepada PPTGWP apabila pengguna berhenti atau bersara. b) Pelawat Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu masuk utama premis premis PPTGWP. Pas ini hendaklah dikembalikan semula selepas tamat lawatan. c) Kehilangan Pas Kehilangan pas mestilah dilaporkan dengan segera.	Pengguna, Pelawat
B07/02 Keselamatan Peralatan	

Perkara	Peranan
B07/02/01 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; b) pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; d) pengguna mesti memastikan perisian *antivirus* bagi semua peralatan ICT yang dibekalkan oleh Jabatan seperti komputer peribadi, *notebook, server* dan lain lain yang berada di bawah tanggungjawab mereka sentiasa aktif (activated) dan dikemas kini di samping turut melakukan imbasan ke atas media storan yang digunakan; e) semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; f) aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang bertanggungjawab. Arahan Keselamatan Kerajaan hendaklah sentiasa dipatuhi bagi mengelak berlakunya kerosakan atau kehilangan aset; g) sekiranya peralatan ICT tidak digunakan, peralatan tersebut hendaklah disimpan di dalam almari atau kabinet atau peti besi atau stor atau bilik khas yang berkunci untuk penyimpanan peralatan ICT; h) peralatan ICT yang kritikal perlu disokong oleh UPS; i) UPS yang berkuasa tinggi perlu diletakkan di bilik yang berasingan bersuhu rendah yang dilengkapi dengan pengudaraan yang sesuai;	Pengguna, Pentadbir Sistem, Pegawai Aset ICT, Penyelaras ICT Bahagian

Perkara	Peranan
j) semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switch, router* dan lain-lain perlu diletakkan di dalam bilik atau rak berkunci; k) semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(*air ventilation*)* yang sesuai; l) peralatan ICT yang hendak dibawa keluar dari premis PPTGWP, perlulah mendapat kelulusan Pegawai Aset ICT atau Penyelaras ICT Bahagian bagi tujuan pemantauan; dan m) aset ICT yang hilang hendaklah dilaporkan mengikut pekeliling perbendaharaan sedia ada.	
B07/02/02 *Clear Desk* Dan *Clear Screen*	
Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer; b) menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c) memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Pengguna
B07/02/03 Media Tandatangan Digital	
Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut:	Pentadbir Sistem, Pengguna

Perkara	Peranan
a) pengguna hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b) tidak boleh dipindah milik atau dipinjamkan; dan c) sebarang kehilangan yang berlaku hendaklah dilaporkan kepada pihak yang dipertanggungjawabkan.	
B07/02/04 Perisian Dan Aplikasi	
Sebarang perisian dan aplikasi yang digunakan hendaklah mematuhi langkah–langkah berikut: a) hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan jabatan; b) lesen perisian (registration code, serials, CD-keys) perlu disimpan berasingan daripada *CD-ROM*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan c) kod sumber (source code) sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan; dan d) sistem aplikasi, perisian dan kod sumber tidak dibenarkan dikongsi, diagih, dibawa keluar atau didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT.	Pengurus ICT, Pegawai Aset ICT, Pentadbir Sistem
B07/02/05 Perkakasan Tanpa Penyeliaan (*Unattended Equipment*)	
Pengguna perlu memastikan mana-mana perkakasan yang ditinggalkan tanpa penyeliaan mematuhi ciri-ciri keselamatan seperti mempunyai kata laluan dan sebagainya. Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.	Pengguna

Perkara	Peranan
B07/02/06 Peralatan Di Luar Premis	
Perkakasan yang dibawa keluar dari premis PPTGWP adalah terdedah kepada pelbagai risiko. Perkakasan yang dibawa keluar premis PPTGWP merangkumi: a) penggunaan perkakasan secara sementara bagi keperluan mesyuarat, latihan dan sebagainya; dan b) penempatan perkakasan secara kekal di sesebuah agensi lain. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) peralatan perlu dilindungi dan dikawal sepanjang masa; dan b) penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pentadbir Sistem
B07/02/07 Pelupusan	
Aset ICT yang hendak dilupuskan perlu mematuhi tatacara pelupusan semasa. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT PPTGWP dilupuskan dengan teratur iaitu: a) pegawai aset ICT akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; b) peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan; c) data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; d) pelupusan peralatan ICT boleh dilakukan secara berpusat atau tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa; e) sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan;	Pegawai Aset ICT, Pengguna

Perkara	Peranan
f) maklumat lanjut berhubung pelupusan boleh dirujuk kepada pekeliling perbendaharaan semasa yang berkuat kuasa; dan g) pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara.	
B07/02/08 Penyelenggaraan	
Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a) mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang di selenggara; b) memastikan perkakasan hanya diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c) menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan d) memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pentadbir Sistem, Pegawai Aset ICT
B07/03 Kawalan Persekitaran	
B07/03/01 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu ke Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil:	Pengurus ICT

Perkara	Peranan
a) menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b) semua ruang pejabat khususnya yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c) peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan 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 berhampiran peralatan komputer; dan g) semua peralatan perlindungan keselamatan dan kebakaran hendaklah di selenggara bagi memastikan ia dapat berfungsi dengan baik.	
B07/03/02 Kabel Rangkaian	
Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan kabel rangkaian: a) semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; b) menggunakan kabel mengikut spesifikasi yang telah ditetapkan; dan c) melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*.	Pentadbir Rangkaian

Perkara	Peranan
B07/03/03 Bekalan Kuasa	
Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: a) semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b) peralatan sokongan seperti UPS dan penjana kuasa *(*power generator*)* boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan c) semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Pengurus ICT
B07/03/04 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Pelan Tindakan dan Kecemasan PPTGWP; dan b) kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Kebakaran yang dilantik mengikut aras.	Pengguna, Pegawai Keselamatan Kebakaran
B07/03/05 Mekanisme Pelaporan Insiden Bukan ICT	
Semua pengguna yang terlibat haruslah melaporkan dan merekodkan sebarang kejadian atau kerosakan peralatan bukan ICT kepada pihak pentadbiran bahagian.	Pengguna
B07/03/06 Mekanisme Kawalan Peralatan Sewaan/POC	
a) Penerimaan Peralatan yang diterima bebas daripada virus, *backdoor, worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT	Pentadbir Sistem

Perkara	Peranan
jabatan. b) Penyelenggaraan i) capaian melalui rangkaian luar PPTGWP adalah tidak dibenarkan; dan ii) aktiviti penyelenggaraan adalah di bawah pengawasan pegawai PPTGWP. c) Pemulangan i) maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (secured delete); dan ii) memastikan semua maklumat jabatan tidak tertinggal pada peralatan.	
B07/03/07 Keselamatan Sistem Dokumentasi	
Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: a) memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada; c) setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar d) pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; e) kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; dan f) menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan, disimpan dan dihantar secara elektronik.	Pentadbir Sistem, Pentadbir Fail

BAHAGIAN 08
KESELAMATAN OPERASI

BAHAGIAN 08	KESELAMATAN OPERASI

Objektif

Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

Perkara	Peranan
B08/01 Prosedur Operasi	
B08/01/01 Pengendalian Dokumen Prosedur Operasi	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) semua prosedur operasi ICT yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap; dan c) semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pentadbir Sistem
B08/01/02 Pengurusan Perubahan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) pengubahsuaian melibatkan perkakasan, sistem pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran Pengurus ICT, pegawai atasan atau pemilik aset ICT terlebih dahulu; b) aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Pentadbir Sistem

Perkara	Peranan
c) semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau sebaliknya.	
B08/01/03 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah dilakukan oleh pegawai yang berlainan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan,kebocoran maklumat terperingkat atau di manipulasi;dan c) perkakasan dan rangkaian yang digunakan bagi tugas membangun, mengemas kini, dan menguji aplikasi hendaklah diasingkan dari perkakasan dan rangkaian yang digunakan di dalam persekitaran pembangunan dan pengujian; peringkat persediaan dan produksi.	Pengurus ICT, Pentadbir Sistem
B08/02 Perancangan Dan Penerimaan Sistem	
B08/02/01 Perancangan Kapasiti	
a) kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan	Pentadbir Sistem

Perkara	Peranan
sistem ICT pada masa akan datang; dan b) keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	
B08/02/02 Penerimaan Sistem	
Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem
B08/03 Perlindungan Daripada Perisian Berbahaya	
B08/03/01 Perlindungan Daripada Malware	
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan malware hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Langkah-langkah pencegahan, pengesanan dan pemulihan bagi memastikan perlindungan aset ICT dari perisian berbahaya adalah seperti berikut: a) memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) mengikut prosedur penggunaan yang betul dan selamat; b) memasang dan menggunakan hanya perisian yang tulen; c) mengimbas semua perisian, sistem, media storan dan kepilan fail dengan *antivirus* yang telah disediakan oleh Jabatan sebelum menggunakannya; d) memastikan paten *antivirus* pada peralatan ICT dikemas kini dengan versi terkini;	Pentadbir Sistem, Pengguna

Perkara	Peranan
e) menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; dan h) mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.	
B08/03/2 Perlindungan Daripada Mobile Code	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan**.**	Pengguna
B08/04 Backup (Sandaran)	
Memastikan salinan backup untuk maklumat, sistem dan perisian sistem disediakan dan diuji secara berkala bagi tujuan kesinambungan perkhidmatan. Backup hendaklah direkodkan dan disimpan secara off-site. Perkara- perkara yang perlu dipatuhi adalah; a) membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu; b) membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi; c) menguji sistem *backup* sedia ada dan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan	Pentadbir Sistem

Perkara	Peranan
d) *backup* dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.	
B08/05 Pengurusan Media	
B08/05/01 Media Storan Mudah Alih	
Penghantaran atau pemindahan media storan mudah alih yang mengandungi maklumat terperingkat ke luar pejabat hendaklah mendapat kebenaran daripada Pengurus ICT terlebih dahulu.	Pengguna
B08/05/02 Prosedur Pengendalian Media	
Di antara proesrosedur-pdur pengendalian media termasuk: a) melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan e) media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut peraturan dan prosedur yang betul dan selamat.	Pentadbir Sistem, Pengguna
B08/06 Paparan Maklumat Umum	

Perkara	Peranan
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat umum adalah seperti berikut: a) memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; b) memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan sebelum dimuat naik ke portal; dan c) memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian.	Pengguna
B08/07 Log Dan Pemantauan	
B08/07/01 Log Peristiwa (Event Log)	
Bertujuan untuk merekodkan dan memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal atau tidak dapat dijelaskan bagi menghasilkan bukti. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log hendaklah direkodkan dan disimpan selaras dengan arahan/pekliling terkini yang dikeluarkan oleh Kerajaan. Fail log hendaklah disimpan untuk tempoh sekurang kurangnya enam (6) bulan. Log hendaklah dikawal bagi mengelakkan integriti data. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti berikut: i. Fail log sistem pengoperasian; ii. Fail log servis (web, e-mel); iii. Fail log aplikasi (audit trail); dan iv. Fail log rangkaian *(*switch, firewall, IPS*)* Perkara-perkara yang perlu dilaksanakan oleh Pentadbir Sistem adalah; a) log audit yang merekodkan semua aktiviti perlu	Pentadbir Sistem

Perkara	Peranan
dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) mewujudkan prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala; c) maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) kesalahan, kesilapan atau penyalahgunaan perlu direkodkan, dianalisis dan diambil tindakan sewajarnya; e) menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan pemulihan/pembaikan dengan segera; f) masa yang berkaitan dengan sistem pemprosesan maklumat dalam PPTGWP perlu diselaraskan dengan sumber waktu yang piawai; dan g) sekiranya terdapat aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, pentadbir sistem hendalah melaporkan kepada pasukan CSIRT PPTGWP	
B08/07/02 Pengauditan Dan Forensik ICT	
CSIRT PPTGWP mestilah bertanggungjawab merekod dan menganalisis: a) sebarang percubaan pencerobohan kepada sistem ICT PPTGWP; b) serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), *spam*, pemalsuan (forgery), pencerobohan (intrusion) ancaman (threats) dan kehilangan fizikal (physical loss); c) pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa	CSIRT PPTGWP, ICTSO, Pentadbir Sistem

Perkara	Peranan
pengetahuan, arahan atau persetujuan mana-mana pihak; d) aktiviti melayari, menyimpan atau mengedar bahan bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e) aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian; g) aktiviti penyalahgunaan akaun e-mel; dan h) aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian. Langkah-langkah yang perlu diambil adalah seperti berikut: a) CSIRT PPTGWP akan menentukan prosedur pengumpulan bahan bukti yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan; b) proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; c) sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan; dan d) semua proses dan hasil siasatan adalah SULIT.	
B08/07/03 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan. Jejak audit hendaklah mengandungi ciri-ciri berikut: a) rekod setiap aktiviti transaksi; b) maklumat jejak audit mengandungi identiti	Pentadbir Sistem

Perkara	Peranan
pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c) aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d) maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Akta Arkib Negara. Pentadbir Sistem hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan	
B08/07/04 Kawalan Audit Sistem Maklumat	
a) Keperluan audit dan sebarang aktiviti pemeriksaan yang melibatkan penentusahan sistem yang beroperasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan perkhidmatan; dan b) Capaian ke atas sistem maklumat semasa pengauditanperlu dikawal selia bagi mengelakkan sebarang penyalahgunaan.	Pentadbir Sistem
B08/07/05 Pengurusan *Technical Vulnerabilities*	
Kawalan terhadap sebarang kelemahan teknikal kepada perkakasan, sistem pengoperasian dan sistem aplikasi perlu diurus secara berkesan, sistematik dan berkala. Perkara-perkara yang perlu dipatuhi adalah: a) Mengenal pasti dan menilai tahap keterdedahan bagi mengenal pasti risiko yang bakal dihadapi; dan	ICTSO, Pentadbir Sistem

Perkara	Peranan
b) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkenaan.	

BAHAGIAN 09
KESELAMATAN KOMUNIKASI

BAHAGIAN 09	KESELAMATAN KOMUNIKASI

Objektif

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

Perkara	Peranan
B09/01 Pengurusan Keselamatan Rangkaian	
B09/01/01 Kawalan Infrastruktur Rangkaian	
Infrastruktur rangkaian perlu dirancang, diurus dan dikawal sebaik mungkin demi melindungi keselamatan maklumat. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: a) polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berkaitan dengan sistem rangkaian; b) peralatan keselamatan komunikasi seperti *firewall* hendaklah dipasang bagi memastikan hak capaian ke atas sistem dapat dilaksanakan seperti ditetapkan; c) sebarang cubaan menceroboh dan aktiviti yang boleh mengancam sistem maklumat PPTGWP perlu dipantau dan dikesan melalui pemasangan peralatan keselamatan komunikasi seperti *Intrusion Prevention Sistem (IPS)*; d) peralatan rangkaian hendaklah diletakkan di lokasi yang bebas dari risiko seperti banjir, gegaran dan habuk; e) sebarang keperluan penyambungan rangkaian hendaklah melalui proses dan prosedur yang ditetapkan; f) penggunaan rangkaian tanpa wayar *(wireless) LAN* di PPTGWP hendaklah mematuhi peraturan yang	Pentadbir Rangkaian

Perkara	Peranan
dikeluarkan oleh pihak berkenaan seperti MAMPU dan Majlis Keselamatan Negara (MKN); dan g) semua perisian berkaitan rangkaian dan keselamatan komunikasi seperti *sniffer* atau *network analyzer* adalah dilarang dipasang pada peralatan ICT kecuali mendapat kebenaran ICTSO.	
B09/01/02 Keselamatan Perkhidmatan Rangkaian	
Perkhidmatan rangakaian hendaklah dipastikan sentiasa selamat bagi menjamin kerahsiaan, integriti dan ketersediaan maklumat. Perkara-perakara yang perlu dipatuhi adalah: a) Mekanisma keselamatan komunikasi, tahap ketersediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara dalaman ataupun menggunakan sumber luar; b) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan komunikasi di bawah kawalan PPTGWP; dan c) Sebarang aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam (PKPA) yang berkuat kuasa perlu disekat melalui penggunaan Web Content Filtering.	Pentadbir Sistem, Pengguna
B09/01/03 Pengasingan Rangkaian	
Pengasingan perkhidmatan rangkaian bertujuan untuk meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara–perkara yang perlu dipatuhi adalah: a) mengenal pasti fungsi dan tanggungjawab Pegawai	Pentadbir Rangkaian dan Keselamatan

Perkara	Peranan
PPTGWP; b) had capaian Pegawai PPTGWP ditentukan mengikut segmen rangkaian berdasarkan keperluan; c) capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada Pegawai PPTGWP yang dibenarkan sahaja; d) Mmengemaskini had capaian Pegawai PPTGWP dari semasa ke semasa mengikut keperluan; dan e) segmen rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaianyang tidak dibenarkan.	
B09/02 Pemindahan Maklumat	
B09/02/01 Prosedur Pemindahan Maklumat	
Prosedur ini bertujuan untuk mengendali, menyimpan, memindah, melindungi maklumat daripada didedah tanpa kebenaran atau salah guna dan memastikan keselamatan pemindahan maklumat dengan entiti luar terjamin. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) mengehadkan dan menentukan capaian kepada Pegawai PPTGWP/Pihak Ketiga yang dibenarkan sahaja; b) mengehadkan perkongsian data untuk tujuan rasmi danyang dibenarkan sahaja; c) polisi, prosedur dan kawalan pemindahan maklumat yang rasmi perlu diwujudkan untuk melindungi pemindahan maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; d) sebarang pemindahan maklumat di antara PPTGWP dan Pihak Ketiga mestilah dikawal; dan e) penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi Kerajaan perlu mendapat kelulusan CIO/Ketua Jabatan.	ICTSO, Pentadbir Sistem, Pengguna

Perkara	Peranan
B09/02/02 Perjanjian Pemindahan Dan Kerahsiaan Maklumat	
a) *Non-Disclosure Agreement* (NDA) perlu diwujudkan bagi memastikan kerahsiaan, integriti dan ketersediaan (CIA) maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara PPTGWP dengan Pihak Ketiga; dan b) Keperluan melindungi keselamatan maklumat yang merangkumi kerahsiaan, integriti dan ketersediaan hendaklah disemak secara berkala dan didokumenkan.	ICTSO, Pentadbir Sistem, Pengguna, Pihak Ketiga
B09/03 Pengurusan Mel Elektronik (E-Mel)	
Maklumat yang dihantar, diterima dan disimpan melalui e-mel PPTGWP perlu dilindungi bagi mengelakkan capaian atau penyebaran maklumat yang tidak dibenarkan. Penggunaan e-mel di PPTGWP hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet. Di antara prosedur-prosedur pengurusan e-mel termasuk: a) menghadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan e-mel *bombing*; b) penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi jabatan sahaja; c) penggunaan e-mel PPTGWP bagi tujuan peribadi adalah tidak dibenarkan; d) perkemasan e-mel hendaklah dibuat sekiranya *mailbox* didapati tidak aktif selama satu (1) bulan kecuali menerima pemakluman rasmi bagi mengesahkan pengguna *mailbox* masih aktif; e) penghantaran lampiran dalam format atau *extension "*.exe, *.bat"* dan " **.com"* tidak dibenarkan; f) hanya warga PPTGWP atau pengguna yang	Pentadbir E-mel, Pengguna

Perkara	Peranan
dibenarkan sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi jabatan; g) Ketua/Ketua Pembantu Tadbir Bahagian perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke PPTGWP di bahagian masing-masing bagi tujuan pengemaskinian e-mel pihak terlibat; h) e-mel rasmi yang dihantar atau diterima hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa; dan i) menggunakan enkripsi bagi dokumen terperingkat yang dihantar secara elektronik.	

BAHAGIAN 10

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

BAHAGIAN 10	PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif

Memastikan sistem yang dibangunkan secara dalaman atau luaran mempunyai ciri-ciri keselamatan ICT yang bersesuaian dan kukuh daripada serangan siber.

Perkara	Peranan
B10/01 Keperluan Keselamatan Sistem Maklumat	
B10/01/01 Analisis Keperluan Dan Spesifikasi Keselamatan Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan; b) Semua sistem maklumat yang dibangunkan sama adasecara dalaman atau luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan berkaitan yang berkuat kuasa; dan c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem maklumat hendaklah mematuhi kawalan keselamatan.	ICTSO, Pentadbir Sistem, Pihak Ketiga
B10/01/02 Perlindungan Perkhidmatan Aplikasi Dalam Rangkaian Awam	
Sistem maklumat yang boleh dicapai melalui rangkaian awam perlu dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat dan pengubahsuaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah: a) identiti penguna/Pihak Ketiga yang diberi tahap capaian perlu dikenal pasti dan disahkan; b) setiap pengguna/Pihak Ketiga perlu diberi peranan mengikut skop dan tanggungjawab yang telah	Pengurus ICT, Pentadbir Sistem, Pengguna, Pihak Ketiga

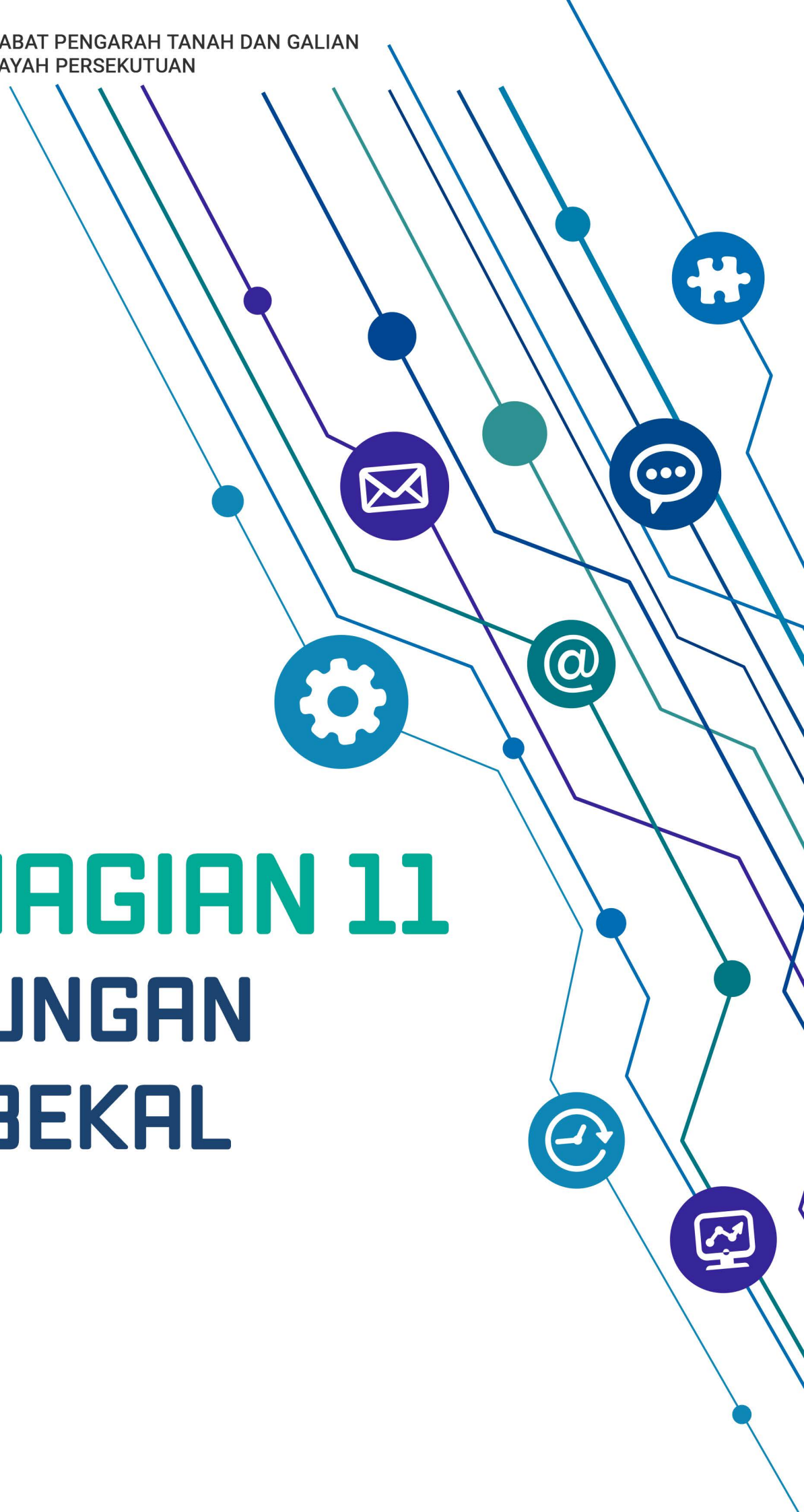
Perkara	Peranan
ditetapkan; dan c) memastikan Pihak Ketiga diberi penerangan mengenai keperluan mematuhi kontrak dan peraturan keselamatan yang ditetapkan dan menandatangani akuan pematuhan PKS.	
B10/01/03 Melindungi Transaksi Perkhidmatan Atas Talian	
a) Maklumat yang terlibat dalam transaksi perkhidmatan atas talian hendaklah dilindungi daripada penghantaran yang tidak lengkap, *misrouting*, pengubahsuaian dan pendedahan yang tidak dibenarkan dan duplikasi; dan b) Sistem pengoperasian dan sistem maklumat hendaklah dilindungi daripada keterdedahan.	Pengurus ICT, Pentadbir Sistem
B10/01/04 Validasi Data Input Dan Output	
Perkara-perkara yang perlu dipatuhi adalah: a) Data input bagi sistem maklumat perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data output daripada sistem maklumat perlu disahkanbagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem, Penguna, Pihak Ketiga
B10/02 Keselamatan Dalam Proses Pembangunan Dan Sokongan	
B10/02/01 Polisi Keselamatan Dan Pembangunan Sistem	
Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan,pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi. Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi dengan membangunkan Dokumen Pelan Pengurusan Keselamatan	Pengurus ICT

Perkara	Peranan
Maklumat (ISMP) semasa proses pembangunan sistem.	
B10/02/02 Prosedur Kawalan Perubahan Sistem	
Prosedur kawalan perubahan hendaklah diwujudkan bagi mengawal sebarang perubahan sepanjang kitar hayat pembangunan sistem maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang ditetapkan dan pelaksanaan hanya mengikut keperluan sahaja; b) perubahan atau pengubahsuaian ke atas perisian dan sistem maklumat hendaklah diuji, didokumenkan dan disahkan sebelum digunakan; dan c) setiap perubahan kepada sistem pengoperasian perlu dikaji dan diuji untuk memastikan tiada sebarang masalah yang timbul.	ICTSO, Pengurus ICT, Pentadbir Sistem, Pemilik Sistem
B10/02/03 Semakan Teknikal Aplikasi Selepas Perubahan Platform Operasi	
Semakan dan pengujian terhadap sistem kritikal perlu dilaksanakan sekiranya berlaku perubahan terhadap sistem pengoperasian bagi memastikan fungsi dan operasi sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) memastikan sistem maklumat, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan; dan b) Ujian penerimaan pengguna perlu dilaksanakan setelahperubahan platform selesai dilaksanakan.	ICTSO, Pengurus ICT, Pentadbir Sistem
B10/02/04 Kawalan Terhadap Perubahan Kepada Perisian	
Sebarang perubahan terhadap perisian adalah tidak digalakkan,kecuali perubahan yang perlu sahaja dan	Pentadbir Sistem

Perkara	Peranan
perubahan tersebut perlu dihadkan	
B10/02/05 Prinsip Kejuruteraan Sistem Yang Selamat	
Prinsip kejuruteraan keselamatan sistem hendaklah dibangunkan, didokumenkan, dikaji dan digunapakai ke atas semua pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteaan hendaklah sentiasa dikaji dari masa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam terkini.	Pentadbir Sistem
B10/02/06 Persekitaran Pembangunan Selamat	
Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem. Secara umumnya kitar hayat pembangunan sistem termasuk skop dan objektif sistem, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian, penerimaan, pemasangan, konfigurasi, penyelenggaraan dan pelupusan. PPTGWP perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; d) Kawalan pemindahan data dari atau ke persekitaran sistem;	Pentadbir Sistem

Perkara	Peranan
e) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	
B10/02/07 Pembangunan Sistem Secara Luaran	
Sebarang aktiviti pembangunan sistem yang melibatkan sumber luar perlu dikawal selia dan dipantau. Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut: 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) PPTGWP hendaklah memastikan *Intellectual property rights (*IPR) dan kod sumber menjadi hak milik PPTGWP/Kerajaan; c) memasukkan klausa ke dalam kontrak yang membenarkan PPTGWP membuat capaian dan melaksanakan semakan terhadap kod sumber; dan d) memasukkan klausa ke dalam kontrak yang membenarkan PPTGWP/Kerajaan mendapat hak pemilikan kod sumber dan melaksanakan pengolahan risiko.	Pengurus ICT, Pentadbir Sistem, Pembekal
B10/02/08 Ujian Keselamatan Sistem	
Aktiviti pengujian penerimaan sistem hendaklah dilaksanakan ke atas sistem baru, naik taraf dan versi baru berdasarkan kriteria yang telah ditetapkan. Bagi memastikan integriti data, pengujian hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan	Pengurus ICT, Pentadbir Sistem

Perkara	Peranan
maklumat iaitu peringkat kemasukan data (*input*), peringkat pemprosesan data (*process*) dan peringkat penjanaan laporan (*output)*. Maklumat lanjut berkaitan dengan pengujian keselamatan sistem boleh merujuk kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam terkini.	
B10/02/09 Ujian Penerimaan Sistem	
Semua sistem maklumat baharu (termasuklah sistem maklumat yang dikemaskini/diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pengurus ICT, Pentadbir Sistem
B10/03 Data Ujian	
B10/03/01 Perlindungan Data Ujian	
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara-perkara yang perlu dipatuhi adalah: a) sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; b) personel yang mempuyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; c) memastikan data sebenar yang disalin ke persekitaran sebenar dilindungi daripada penyalahgunaan atau dipadam sebaik sahaja pengujian selesai; dan d) mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	Pengurus ICT



BAHAGIAN 11
HUBUNGAN PEMBEKAL

BAHAGIAN 11	HUBUNGAN PEMBEKAL

Objektif

Memastikan aset ICT PPTGWP yang boleh dicapai oleh pembekal dilindungi. Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa.

Perkara	Peranan
B11/01 Keselamatan Maklumat Dalam Hubungan Pembekal	
B11/01/01 Polisi Keselamatan Maklumat Ke Atas Pembekal	
Keperluan keselamatan mekalumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset PPTGWP. Perkara-perkara yang perlu dipatuhi adalah: a) pembekal hendaklah menandatangani Borang Akuan (Akta Berkanun 1960) PPTGWP; b) pembekal hendaklah menandatangani Borang Akuan Pematuhan Polisi Keselamatan Siber (PKS) PPTGWP;; c) pembekal hendaklah menjalani ujian tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); dan d) pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas.	Pengurus ICT, Pembekal
B11/01/02 Kawalan Keselamatan Maklumat Melalui Perjanjian	
Perjanjian dengan pihak pembekal hendaklah merangkumi keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan perkhidmatan teknologi maklumat dan komunikasi.	CIO, Pengurus ICT, Pembekal

Perkara	Peranan
B11/01/03 Kawalan Keselamatan Maklumat Dengan Pembekal Utama Kepada Pihak Ketiga	
Perjanjian dengan Pihak Ketiga hendaklah meliputi risiko keselamatan yang merangkumi perkhidmatan ICT dan kesinambungan bekalan produk dengan pembekal utama kepada Pihak Ketiga.	Pengurus ICT, ICTSO, Pihak Ketiga
B11/02 Pengurusan Penyampaian Perkhidmatan Pembekal	
B11/02/01 Pemantauan Dan Penilaian Perkhidmatan Pembekal	
PPTGWP hendaklah memantau, menyemak dan mengaudit perkhidmatan Pihak Ketiga secara berkala bagi mengekalkan tahap keselamatan maklumat adalah sama seperti yang dipersetujui dalam perjanjian dengan Pihak Ketiga.	Pengurus ICT, ICTSO
B11/02/02 Pengurusan Perubahan Perkhidmatan Pembekal	
Setiap perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut SOP yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) perubahan di dalam perjanjian bersama pembekal; b) perubahan yang dilakukan oleh PPTGWP 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

BAHAGIAN 12
PENGURUSAN INSIDEN KESELAMATAN ICT

BAHAGIAN 12	PENGURUSAN INSIDEN KESELAMATAN ICT

Objektif

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

Perkara	Peranan
B12/01 Pengurusan Insiden Dan Penambahbaikan Keselamatan Maklumat	
B12/01/01 Tanggungjawab Dan Prosedur	
Prosedur bagi mengurus insiden keselamatan ICT perlu diwujudkan dan didokumenkan. PPTGWP bertanggungjawab dalam pengurusan pengendalian insiden keselamatan ICT.	Pasukan CSIRT PPTGWP
B12/01/02 Pelaporan Insiden Keselamatan Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada Pasukan CSIRT PPTGWP. Semua maklumat adalah SULIT dan tidak boleh didedahkan tanpa kebenaran daripada ICTSO; b) mematuhi prosedur operasi standard (SOP) keselamatan ICT PPTGWP; c) mengenal pasti semua jenis insiden keselamatan ICT 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 PPTGWP
B12/01/03 Pelaporan Kelemahan Keselamatan Maklumat	

Perkara	Peranan
Insiden keselamatan siber adalah meliputi perkara-perkara berikut: a) *Pelanggaran Polisi (Violation of Policy)* Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar PKS. b) *Penghalangan Penyampaian Perkhidmatan (*Denial of Service*)* Ancaman ke atas keselamatan sistem maklumat komputer iaitu perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal termasuklah *Denial of Service* (DoS), *Distributed Denial of Service* (DDoS) dan sabotaj. c) *Pencerobohan (Intrusion)* Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem maklumat tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem maklumat, pindaan data dan pindaan kepada konfigurasi sistem maklumat. d) Pemalsuan (*Forgery*) Pemalsuan dan penyamaran identiti yang dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti dan maklumat serta penipuan. e) *Spam* Spam adalah e-mel yang dihantar ke akaun orang lain oleh penghantar yang tidak dikenali dalam satu lain masa dan secara berulang kali. Ini menyebabkan kesesakan dan tindak balas	Pasukan CSIRT, Pengguna

Perkara	Peranan
rangkaian menjadi perlahan. f) *Malicious Code* Perisian atau kod pengaturcaraan yang dimasukkan ke dalam sistem maklumat tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware, adware* dan sebagainya g) *Harrasment/Threats* Gangguan dan ancaman melalui e-mel, media sosial dan media elektronik yang bermotifkan personal/peribadi dan atas sebab tertentu. h) *Attempts/Hack Threats/Information Gathering* Percubaaan (samada gagal atau berjaya) untuk mencapai sistem maklumat atau data tanpa kebenaran. Termasuk sniffing, *spoofing, phishing, probing, war driving* dan *scanning.* i) Kehilangan Fizikal (*Physical Lost*) Kehilangan capaian disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.	
B12/01/04 Penilaian Dan Keputusan Insiden Keselamatan Maklumat	
PPTGWP hendaklah menilai sama ada serangan diklasifikasikan sebagai insiden. Tindakan ke atas insiden yang dilaporkan akan dibuat berasaskan tahap kritikal sesuatu insiden dan keutamaan keutamaan akan ditentukan seperti berikut: a) <u>Keutamaan 1</u> Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara. b) <u>Keutamaan 2</u>	ICTSO, Pasukan CSIRT PPTGWP

Perkara	Peranan
i) Pencerobohan atau percubaan menceroboh melalui infrastruktur internet ke atas peralatan rangkaian; ii) Penghalangan penyampaian perkhidmatan secara teragih (*Distributed Denial of Service*); iii) Serangan atau kelemahan terbaru (*New Vulnerabilities*); iv) Pencerobohan melalui pemalsuan identiti; v) Pengubahsuaian laman web, perisian, atau mana-mana komponen sistem maklumat tanpa pengetahuan, arahan atau persetujuan pihak yang berkenaan; dan vi) Gangguan sistem maklumat untuk pemprosesan data atau penyimpanan data tanpa kebenaran.	
B12/01/05 Tindak Balas Terhadap Insiden Keselamatan Maklumat	
Tindak balas insiden keselamatan hendaklah ditangani berdasarkan prosedur Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam terkini.	ICTSO, Pasukan CSIRT PPTGWP
B12/01/06 Pengumpulan Dan Pengendalian Bukti	
Maklumat mengenai insiden keselamatan siber perlu dikenalpasti, dikumpul, dianalisis dan disimpan bagi tujuan pengumpulan dan pengendalian bukti. Pasukan CSIRT PPTGWP hendaklah memastikan bahan bukti berkaitan insiden keselamatan siber dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan bukti seperti jejak audit, *backup* berkala dan *off-site backup* hendaklah mengikut atacara pengendalian yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i) melindungi integriti bahan bukti;	Pengurus ICT, ICTSO, Pasukan CSIRT PPTGWP

Perkara	Peranan
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.	

BAHAGIAN 13

KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

BAHAGIAN 13	KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif

Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

Perkara	Peranan
B13/01 Kesinambungan Perkhidmatan Maklumat	
Ketua Jabatan bertanggungjawab memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT PPTGWP. PPTGWP hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya semasa krisis atau bencana. PPTGWP perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi PPTGWP, keperluan dan ekspektasi pihak-pihak berkepentingan, undang-undang dan peraturan yang terpakai dalam merancang kesinambungan keselamatan maklumat.	PTG
B13/02 Pelan Kesinambungan Perkhidmatan (PKP)	
Pelan Pemulihan Bencana hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini perlulah mendapat perakui oleh Ketua Jabatan dan perkara-perkara berikut perlu diberi perhatian:	CIO, Koordinator PKP

Perkara	Peranan
a) melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) atau Pasukan Pemulihan Bencana PPTGWP; b) menetapkan polisi PKP; c) mengenalpasti perkhidmatan kritikal; d) melaksanakan Kajian Impak Perkhidmatan (Business Impact Analysis – BIA) dan penilaian risiko terhadap perkhidmatan kritikal; e) membangunkan Pelan Induk Pengurusan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana ICT; f) 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; g) melaksanakan program kesedaran dan latihan kepada pengguna mengenai prosedur kecemasan; h) mengkaji dan mengemas kini pelan sekurang kurangnya setahun sekali; dan i) mewujudkan Pusat Pemulihan Bencana di lokasi lain.	
B13/03 Perubahan Atau Pengecualian PKP	
Sekiranya terdapat perubahan/pengemaskinian atau pengecualian yang perlu dilakukan, permintaan secara bertulis termasuk keterangan dan kebenaran untuk pengecualian/perubahan hendaklah dikemukakan kepada	CIO, Koordinator PKP
B13/04 Program Latihan Dan Kesedaran Terhadap PKP	
Semua pegawai dan kakitangan PPTGWP perlu mempunyai kesedaran dan mengetahui peranan masing-masing terhadap PKP. Ketua Jabatan bertanggungjawab dalam memastikan latihan dan program kesedaran	CIO, Koordinator PKP

Perkara	Peranan
terhadap PKP dilaksanakan setiap tahun.	
B13/05 Pengujian PKP	
a) PKP perlulah diuji dua (2) tahun sekali atau selepas perubahan utama, atau yang mana terdahulu bagi memastikan semua pihak yang berkenaan mengetahui dan maklum akan pelaksanaannya; b) Salinan PKP mestilah disimpan di lokasi berasingan bagi mengelakkan kerosakan akibat bencana di lokasi utama. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; c) Ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan; d) Kementerian/Jabatan/Agensi hendaklah memastikan salinan Pelan Kesinambungan Perkhidmatan sentiasa dikemas kini dan dilindungi seperti di lokasi utama; dan e) Komponen PKP seperti Pelan Pemulihan Bencana (Disaster Recovery Plan – DRP), Pelan Komunikasi Krisis (Crisis Communication Plan – CCP) dan Pelan Tindak Balas Kecemasan (Emergency Response Plan – ERP) perlu diuji dua (2) tahun sekali atau selepas perubahan utama, atau yang mana terdahulu.	PTG, Koordinator PKP, Pasukan Pemulihan Bencana
B13/06 Ketersediaan Kemudahan Pemprosesan Maklumat	
Semua sistem maklumat dan peralatan yang kritikal hendaklah mempunyai kemudahan redundancy dan diuji (failover test) keberkesanannya mengikut keperluan	Pasukan Pemulihan Bencana

BAHAGIAN 14
PEMATUHAN

BAHAGIAN 14	PEMATUHAN

Objektif

Meningkatkan dan memantapkan tahap keselamatan siber bagi menghindari pelanggaran undang-undang, kewajipan berkanun , peraturan atau ikatan kontrak yang berkaitan dengan keselamatan maklumat.

Perkara	Peranan
B14/01 Pematuhan Polisi	
Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan bahawa pematuhan dan sebarang perlanggaran dielakkan. Langkah-langkah perlu bagi mengelakkan sebarang perlanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Polisi Keselamatan Siber PPTGWP dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.	PTG
B14/02 Keperluan Perundangan	
Senarai perundangan dan peraturan yang berkuat kuasa dari semasa ke semasa yang perlu dipatuhi oleh semua pegawai dan kakitangan PPTGWP adalah seperti di **Lampiran A**.	Pegawai dan Kakitangan PPTGWP
B14/03 Perlindungan Dan Privasi Data Peribadi	
Pegawai dan kakitangan PPTGWP perlu sedar bahawa data kegunaan peribadi yang dijana dalam aset ICT adalah milik PPTGWP. Pihak pengurusan tidak menjamin kerahsiaan data peribadi yang disimpan dalam aset ICT. Untuk tujuan keselamatan dan penyelenggaraan rangkaian, pegawai yang diberi kuasa perlu mengawasi peralatan, sistem dan rangkaian. Pihak pengurusan PPTGWP berhak mengaudit rangkaian dan sistem secara berkala bagi memastikan ia mematuhi PKS PPTGWP.	Pegawai dan Kakitangan PPTGWP

Perkara	Peranan
PPTGWP menggalakkan dasar privasi yang adil. Pihak pengurusan perlu bertanggungjawab bagi memastikan semua maklumat peribadi digunakan berdasarkan keperluan untuk mengelakkan penyalahgunaan maklumat. Pendedahan maklumat peribadi tentang pegawai dan kakitangan PPTGWP kepada pihak ketiga tidak sepatutnya berlaku kecuali: 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 mencukupi seperti yang ditentukan oleh Unit Undang-undang serta perjanjian jelas diperoleh daripada pengurusan sumber manusia;dan d) Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pengeluaran yang tidak sah mengikut undang-undang, peraturan, kontrak dan keperluan PPTGWP.	
B14/04 Semakan Keselamatan Maklumat	
Semakan keselamatan maklumat mestilah diambil kira seperti berikut: 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 meminimakan ancaman dan meningkatkan ketersediaan sistem; dan c) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian	Pengurus ICT, ICTSO

Perkara	Peranan
berlaku gangguan dalam penyediaan perkhidmatan.	
B14/05 Pelanggaran Perundangan	
Mengambil tindakan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan termasuk Polisi Keselamatan Siber yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972. Antara tindakan yang boleh diambil terhadap pihak ketiga adalah penamatan kontrak.	PTG, UI, PUU
B14/06 Akuan Pematuhan Polisi Keselamatan Siber	
Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan semua pegawai dan kakitangan PPTGWP dan Pihak Ketiga menandatangani Akuan Pematuhan Polisi Keselamatan Siber seperti di **Lampiran B**.	PTG, Pegawai dan Kakitangan PPTGWP, Pihak Ketiga
B14/07 Pematuhan Terhadap Hak Harta Intelek	
Prosedur pengawalan hendaklah dilaksanakan bagi memastikan pematuhan kepada perundangan, peraturan dan keperluan kontrak berkaitan produk yang mempunyai IPR termasuk perisian *proprietary*.	Pengurus ICT, ICTSO

PEJABAT PENGARAH TANAH DAN GALIAN
WILAYAH PERSEKUTUAN

TERMA DAN TAFSIRAN

TERMA DAN TAFSIRAN

TERMA	TAFSIRAN
Antivirus	Perisian yang mengimbas virus pada media storan, seperti cakera keras (hard disk), *external hard disk* dan *USB drive* untuk sebarang kemungkinan adanya virus.
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari suatu tempat ke suatu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
Aset ICT	Peralatan ICT termasuk komputer, media storan, *server, router, firewall*, rangkaian dan lain-lain.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh: di antara cakera keras dan PC utama) dalam jangka masa yang ditetapkan.
Cyber Security Incident Respond Team (CSIRT)	*Cyber Security Incident Respond Team (CSIRT)* ialah pasukan tindak balas insiden keselamatan siber.
Chief Information Officer (CIO)	Ketua Pegawai Maklumat yang bertanggungjawab terhadap keselamatan ICT.
Chief Digital Officer (CDO	Ketua Pegawai Digital yang bertanggungjawab terhadap pelaksanaan inisiatif dan perkhidmatan pendigitalan.
Clear Desk dan *ClearScreen*	Tidak meninggalkan dokumen data dan maklumat terperingkat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.

TERMA	TAFSIRAN
Denial of service	Halangan pemberian perkhidmatan.
Disaster Recovery Center (DRC)	Pusat Pemulihan Bencana.
Encryption	Enkripsi atau penyulitan. Proses enkripsi data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
Information and Communication Technology (ICT)	Teknologi Maklumat dan Komunikasi
ICT Security Officer (ICTSO)	Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan adalah perisian atau perkakasan yang dapat mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.

TERMA	TAFSIRAN
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Berperanan bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Sebagai contoh, *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
Local Area Network (LAN)	Rangkaian kawasan setempat yang menghubungkan komputer.
Malicious Code	Perisian hasad atau jahat yang memasuki sistem komputer dan menyebabkan risiko keselamatan seperti kerosakan komputer, gangguan capaian Internet dan sebagainya tanpa disedari oleh pengguna.
MODEM	Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Mobile Code	Perisian yang boleh dipindahkan antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar Internet.
National Cyber Security Agency (NACSA)	Agensi Keselamatan Siber Negara berperanan menjamin dan mengukuhkan daya tahan Malaysia dalam menghadapi ancaman serangan siber, dengan menyelaras dan menyatukan pakar dan sumber terbaik negara dalam bidang keselamatan siber.
Pengguna	Pegawai/kakitangan PPTGWP dan pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT PPTGWP.

TERMA	TAFSIRAN
Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan daripada segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
Pengurus ICT	Pegawai yang mengetuai organisasi ICT di Bahagian/Jabatan/Kementerian.
Pihak Luaran	Terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan atau pelawat yang mengunjungi PPTGWP atas urusan rasmi.
Public Key Infrastructure (PKI)	Infrastruktur Kunci Awam
Penilaian Risiko	Penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
PUU	Pegawai Undang-Undang
Restoration	Proses penarikan semula data.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ia tidak digunakan dalam jangka masa tertentu.
Server	Pelayan.
Switch	Alat yang boleh menapis (*filter*) dan memajukan (*forward*) isyarat paket data antara segmen rangkaian LAN.

TERMA	TAFSIRAN
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
UI	Unit Integriti
Uninterruptible Power Supply (UPS)	Peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wide Area Network (WAN)	Rangkaian yang merangkumi kawasan yang luas.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
Worm	Sejenis virus yang boleh beraplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

LAMPIRAN

SENARAI PERUNDANGAN DAN PERATURAN

BIL.	SENARAI PERUNDANGAN DAN PERATURAN
1	1Pekeliling Perbendaharaan AM 2 Tahun 2018 : Tatacara Pengurusan Aset Alih Kerajaan
2	Akta Tandatangan Digital 1997
3	Akta Rahsia Rasmi 1972
4	Akta Jenayah Komputer 1997
5	Akta Hak cipta (Pindaan) Tahun 1997
6	Akta Komunikasi dan Multimedia 1998
7	Akta 709 – Akta Perlindungan Data Peribadi 2010
8	Akta 658 – Akta Perdagangan Elektronik 2006
9	Akta 629 – Akta Arkib Negara 2003
10	Arahan Keselamatan
11	Arahan Perbendaharaan
12	Arahan Teknologi Maklumat 2007
13	Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara
14	Arahan 24 – Dasar dan Mekanisme Pengurusan Krisis Siber Negara
15	Dasar Pengurusan Rekod dan Arkib Elektronik
16	Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU)
17	Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam
18	Garis Panduan Pengurusan Rekod
19	Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan

BIL.	SENARAI PERUNDANGAN DAN PERATURAN
	Pembangunan Sistem Aplikasi
20	Pekeliling Am Bilangan 3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
21	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 : Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan
22	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 : Panduan Pengurusan Pejabat
23	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 : Pengurusan Laman Web Agensi Sektor Awam
24	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 : Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)]
25	Pekeliling Am Bilangan 1 Tahun 2015 : Pelaksanaan Data Terbuka Sektor Awam
26	Pekeliling Transformasi Pentadbiran Awam Bilangan 3 Tahun 2017 : Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan
27	Pekeliling Am Bilangan 4 Tahun 2022 : Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam
28	Pekeliling Perbendaharaan Malaysia Terkini : Kaedah Perolehan Kerajaan dan Pengurusan Kontrak
26	Perintah-Perintah Am
30	Pelan Pemulihan Bencana ICT PPTGWP
31	PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua)
32	Polisi Keselamatan Siber Sektor Awam (MAMPU)
33	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)
34	Surat Pekeliling Am Bilangan 2/1987 : Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987)

BIL.	SENARAI PERUNDANGAN DAN PERATURAN
35	Surat Arahan KPPA bertarikh 28 Januari 2015 : Tindakan Ke Atas Penjawat Awam Yang Mendedahkan / Membocorkan Dokumen / Maklumat Terperingkat Kerajaan
36	Surat Pekeliling Am Bilangan 6 Tahun 2005 : Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam
37	Surat Arahan Ketua Setiausaha Negara bertarikh 20 Oktober 2006 : Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-Agensi Kerajaan
38	Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 : Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan yang
39	Surat Arahan Ketua Pengarah MAMPU bertarikh 24 November 2010 : Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat
40	Surat Arahan Ketua Pengarah MAMPU bertarikh 22 Januari 2010 : Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam
41	Surat Pekeliling Am Bilangan 3 Tahun 2015 : Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek ICT Agensi Sektor Awam

AKAUN PEMATUHAN
POLISI KESELAMATAN SIBER
PEJABAT PENGARAH TANAH DAN GALIAN WILAYAH PERSEKUTUAN

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian/Unit : .....

Jabatan/Agensi : .....

Adalah saya dengan sesungguhnya dan sebenarnya mengaku bahawa:

i) Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber Pejabat Pengarah Tanah dan Galian Wilayah Persekutuan; dan

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

Tandatangan :

Tarikh :

* Polisi Keselamatan Siber PPTGWP boleh dicapai menerusi Portal Rasmi PPTGWP.

AKAUN PEMATUHAN
POLISI KESELAMATAN SIBER
PEJABAT PENGARAH TANAH DAN GALIAN WILAYAH PERSEKUTUAN
(PEMBEKAL/PIHAK KETIGA)

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Syarikat/Organisasi : .....

No. Kontrak (Jika Ada) : .....

Adalah saya dengan sesungguhnya dan sebenarnya mengaku bahawa:

iii) Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber Pejabat Pengarah Tanah dan Galian Wilayah Persekutuan; dan

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

Tandatangan :

Tarikh :

Pengesahan Pegawai Keselamatan ICT PPTGWP

.....

(Tandatangan dan Cop Jawatan)

Tarikh :

* Polisi Keselamatan Siber PPTGWP boleh dicapai menerusi Portal Rasmi PPTGWP.

BORANG AKUAN
PEJABAT PENGARAH TANAH DAN GALIAN WILAYAH PERSEKUTUAN
(Akta Akuan Berkanun 1960)

Saya .....

No. Kad Pengenalan .....

Jawatan .....

beralamat di .....

..... dengan sesungguhnya dan sebenarnya mengakui bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta tersebut, khususnya :

i. saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu rahsia atau apa-apa tingkah laku yang merbahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

ii. saya juga faham bahawa segala maklumat rasmi yang saya perolehi dari mana-mana jabatan kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan **Pejabat Pengarah Tanah dan Galian Wilayah Persekutuan Kuala Lumpur** dengan tidak terlebih dahulu mendapat kebenaran bertulis daripada pihak berkuasa yang berkenaan.

Saya membuat akuan ini dengan kepercayaan bahawa apa-apa yang tersebut di dalamnya adalah benar, serta menurut peruntukan **Akta Akuan Berkanun 1960**.

Diperbuat dan dengan sebenar-benarnya diakui oleh yang tersebut namanya di atas ……
.....
di .....
di Negeri .....
pada .....haribulan....., 20.....

Di-hadapan saya,

……
(*Tandatangan Hakim Mahkamah Sesyen, Majistret atau Pesuruhjaya Sumpah)*

Cop Meterai

Pejabat Pengarah Tanah dan Galian
Wilayah Persekutuan Kuala Lumpur

SCAN ME

Become a friend
Pejabat Pengarah Tanah & Galian WP

Follow us
PPTG WP @pptg_wp

Watch our videos
Pejabat Pengarah Tanah & Galian WP