DASAR KESELAMATAN ICT (DKICT)

VERSI 4.0 | 17 NOVEMBER 2020

JABATAN PENDAFTARAN PERTUBUHAN MALAYSIA

REKOD PINDAAN

TARIKH	VERSI	BAB/MUKA SURAT	BUTIRAN PINDAAN
03/11/2013	1.0	Keseluruhan dokumen	Dokumen asal
17/05/2015	2.0	21, 26	Kemaskini Perkara berikut: DKICT JPPM-0202 Struktur Organisasi, DKICT JPPM-0205 Keselamatan Maklumat dalam Pengurusan Projek
12/07/2017	3.0	Keseluruhan dokumen	Kemaskini kawalan-kawalan berdasarkan standard ISO/IEC 27001:2013
17/11/2020	4.0	Keseluruhan dokumen	Kemaskini perkara berikut: • Muka depan • Skop • Prinsip-prinsip: a) Akses atas dasar perlu mengetahui • 1.1.3 Penyelenggaraan Dasar • 1.1.4 Pengecualian Dasar • 2.1 Infrastruktur Organisasi Dalaman • 2.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga • 2.2.3 Polisi Keselamatan Maklumat berkaitan Hubungan Pembekal • 2.2.4 Rangkaian Pembekal ICT • 4.1.2 Dalam Perkhidmatan • 5.1.2 Kawalan Masuk Fizikal • 5.2.1 Peralatan ICT • 5.2.2 Media Storan • 5.2.5 Penyelenggaraan Peralatan ICT • 5.2.7 Pelupusan Peralatan ICT • 5.3.1 Kawalan Persekitaran • 5.3.4 Prosedur Kecemasan • 6.1.2 Kawalan Perubahan • 6.1.3 Pengasingan Tugas dan Tanggungjawab • 6.6.1 Kawalan Infrastruktur Rangkaian • 6.8.2 Penggunaan Mel Elektronik (E-mel) • 6.8.3 *Bring Your Own Device* (BYOD) • 6.10.1 Pengauditan dan Forensik ICT • 6.10.2 Jejak Audit • 7.2.3 Pengurusan Kata Laluan • 7.2.4 *Clear Desk & Clear Screen*

TARIKH	VERSI	BAB/MUKA SURAT	BUTIRAN PINDAAN
			• 10.1.1 Pelan Kesinambungan Perkhidmatan • 11.1.5 Pelanggaran Dasar • Glosari • Lampiran 1: Surat Akuan Pematuhan DKICT JPPM • Lampiran 2: Senarai Perundangan dan Peraturan

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT (DKICT) JPPM mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT JPPM.

OBJEKTIF

Dasar Keselamatan ICT JPPM diwujudkan untuk menjamin kesinambungan urusan JPPM dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi JPPM. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Objektif utama keselamatan ICT JPPM adalah seperti berikut:

a) Memastikan kelancaran operasi JPPM dan meminimumkan kerosakan atau kemusnahan;
b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari segi kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
c) Mencegah salah guna atau kecurian asset ICT Kerajaan.

PERNYATAAN DASAR

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.

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 dari sumber yang sah.

Dasar Keselamatan ICT JPPM 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 kemas 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) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Aset ICT JPPM terdiri daripadaperalatan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT JPPM menetapkan keperluan-keperluan asas berikut:

a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT JPPM 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) Perkakasan

Semua asset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan JPPM. 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 di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada JPPM;

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 JPPM. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod JPPM, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkid dan lain-lain;

e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian JPPM 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 perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT JPPM 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.

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 JPPM hendaklah menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan 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 terperingkat 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, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi asset ICT daripada kesilapan, kebocoran maklumat terperingkat 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, , *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f) Pematuhan

Dasar Keselamatan ICT JPPM 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

JPPM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu JPPM 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.

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat JPPM 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.

JPPM 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.

JPPM perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b) menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
c) mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
d) memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak- pihak lain yang berkepentingan.

BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

1.1 Dasar Keselamatan ICT

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan JPPM dan perundangan yang berkaitan.

1.1.1 Pelaksanaan Dasar

Pelaksanaan dasar ini dilaksanakan oleh Ketua Pegawai Maklumat (CIO) dan disokong oleh Jawatankuasa Pemandu ICT.

CIO

1.1.2 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna JPPM (termasuk kakitangan, pembekal, pakar runding dan lain-lain).

CIO/ICTSO

1.1.3 Penyelenggaraan Dasar

Dasar Keselamatan ICT JPPM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT JPPM: a) Kenal pasti dan tentukan perubahan yang diperlukan; b) Kemuka cadangan pindaan dan memaklumkan kepada Jawatankuasa Pemandu ICT JPPM dan dibawa ke dalam Mesyuarat Jawatankuasa Pemandu ICT JPPM untuk kelulusan; dan c) Dasar ini hendaklah dikaji semula sekurang-kurangnya dua (2) tahun sekali atau mengikut keperluan semasa.	CIO/ICTSO

1.1.4 Pengecualian Dasar

Dasar Keselamatan ICT JPPM adalah terpakai kepada semua pengguna JPPM dan tiada pengecualian diberikan.	Semua

BIDANG 02 ORGANISASI KESELAMATAN

2.1 Infrastruktur Organisasi Dalaman

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT JPPM.

2.1.1 Ketua Pengarah JPPM

Ketua Pengarah JPPM adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: — Ketua Pengarah JPPM

a) Memantau pelaksanaan dasar keselamatan maklumat di JPPM melalui Ketua Pegawai Maklumat (CIO);
b) Memastikan sumber keperluan organisasi berkaitan pelaksanaan keselamatan maklumat adalah mencukupi; dan
c) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT JPPM.

2.1.2 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) berperanan dan bertanggungjawab seperti berikut: — CIO

a) Memantau pelaksanaan Pelan Strategik Teknologi Maklumat JPPM yang mengandungi perancangan penggunaan ICT dalam menyokong pencapaian matlamat JPPM;
b) Memperkenalkan dan menyepadukan proses-proses yang cross functional antaran Jabatan bagi menghasilkan perkhidmatan yang lebih cekap dan berkesan;
c) Menyelaras pembangunan, pengendalian dan pengurusan sistem dan infrastruktur ICT yang utuh dan selamat serta

berdasarkan kepada ciri modular, connectivity, inter-operability dan portability;

d) Menentukan hala tuju sistem aplikasi JPPM bagi mengurangkan masa dan kos pembangunan, penyelenggaraan dan pengoperasian;
e) Memelihara integriti data elektronik, menggalak perkongsian maklumat dan menyediakan kaedah bagi penyebaran maklumat secara elektronik kepada pengguna-penguna yang sah sama ada dalam atau luar JPPM;
f) Menganggotai Jawatankuasa Perancangan dan Pembangunan atau Jawatankuasa Utama yang menggubal dasar dan bertanggungjawab terus kepada Ketua Pengararah JPPM;
g) Mempromosikan kegunaan ICT yang berkesan dan seiringan untuk mencapai matlamat strategik JPPM dan bertindak sebagai agen dan perintis perubahan (Champion of Change); dan
h) Memimpin dan melibatkan JPPM dalam usaha-usaha Kerajaan untuk membangun dan melaksanakan projek ICT Sektor Awam yang membawa dalam pengurusan dan pentadbiran Perkhidmatan Awam.

2.1.3 Pegawai Keselamatan ICT (ICTSO)

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: ICTSO

a) Memastikan semua infrastruktur keselamatan ICT JPPM menepati prinsip-prinsip keselamatan berpandukan Rangka Dasar Keselamatan ICT dan Arahan Keselamatan Kerajaan;
b) Menyediakan dan mengkaji semula dokumen infrastruktur keselamatan ICT JPPM bagi tujuan audit keselamatan ICT;
c) Mengenalpasti bidang-bidang keselamatan ICT JPPM yang perlu diberikan perhatian;
d) Memastikan tahap keselamatan ICT JPPM adalah terjamin

setiap masa;

e) Memastikan semua warga JPPM memahami keperluan standard, garis panduan dan prosedur keselamatan di bawah Rangka Dasar Keselamatan ICT Kerajaan;

f) Menjalankan penilaian risiko dan program-program keselamatan ICT di JPPM;

g) Mewujudkan pelan tindakan bagi mengurus risiko akibat daripada ketidakpatuhan kepada standard, garis panduan dan prosedur keselamatan ICT di JPPM;

h) Melaporkan kepada CERT JPPM, CERT KDN seterusnya GCERT NACSA mengenai sebarang insiden keselamatan ICT yang berlaku di JPPM;

i) Membantu dalam membangunkan standard, garis panduan dan prosedur untuk aplikasi, sistem dan infrastruktur ICT di JPPM bagi mematuhi keperluan Dasar Keselamatan ICT KDN;

j) Mewujudkan program-program bagi meningkatkan pengetahuan, kesedaran dan pembudayaan mengenai teknologi dan mekanisme kawalan maklumat dan aset ICT, ancaman-ancaman siber serta peranan dan tanggungjawab pengguna dalam mengendalikan kemudahan ICT di JPPM;

k) Menyebarkan dan menyalurkan amaran awal terhadap ancaman-ancaman yang berpotensi menyebabkan kerosakan besar kepada aset ICT JPPM; dan

l) Mengurus keseluruhan program-program keselamatan ICT di JPPM.

2.1.4 Pentadbir Sistem ICT

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: Pentadbir Sistem ICT

a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT JPPM;
c) Memantau aktiviti capaian harian sistem aplikasi pengguna;
d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; dan
e) Menganalisis dan menyimpan rekod jejak audit.

2.1.5 Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti Pengguna berikut:

a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPPM;
b) Mengetahui dan memahami implikasi keselamatan ICT daripada tindakannya;
c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;
d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT JPPM dan menjaga kerahsiaan maklumat JPPM;
e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;
f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan
g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT JPPM sebagaimana **Lampiran 1**.

2.1.6 Jawatankuasa Pemandu ICT JPPM

Jawatankuasa Keselamatan ICT JPPM

Jawatankuasa Pemandu ICT JPPM adalah jawatankuasa yang bertanggungjawab dalam memantau dan menyokong pelaksanaan berkaitan keselamatan maklumat di JPPM.

Keanggotaan Jawatankuasa Pemandu ICT JPPM adalah seperti berikut:

Pengerusi: Ketua Pengarah

Ahli:

1. Timbalan Ketua Pengarah (CIO JPPM)
2. Pengarah BPTM (ICTSO)
3. Pengarah-Pengarah Bahagian JPPM Ibu Pejabat
4. Pengarah-Pengarah JPPM Negeri
5. Wakil BPTM

Urusetia bagi Jawatankuasa Pemandu ICT JPPM adalah Bahagian Pengurusan Teknologi Maklumat (BPTM).

Bidang Kuasa:

a) Memastikan semua infrastruktur keselamatan ICT JPPM menepati prinsip-prinsip keselamatan berpandukan Rangka Dasar Keselamatan ICT dan Arahan Keselamatan Kerajaan;
b) Menyediakan dan mengkaji semula dokumen infrastruktur keselamatan ICT JPPM bagi tujuan audit keselamatan ICT;
c) Mengenalpasti bidang-bidang keselamatan ICT JPPM yang perlu diberikan perhatian;
d) Memastikan tahap keselamatan ICT JPPM adalah terjamin setiap masa;
e) Memastikan semua warga JPPM memahami keperluan standard, garis panduan dan prosedur keselamatan di bawah Rangka Dasar Keselamatan ICT Kerajaan;

f) Menjalankan penilaian risiko dan program-program keselamatan ICT di JPPM;

g) Mewujudkan pelan tindakan bagi mengurus risiko akibat daripada ketidakpatuhan kepada standard, garis panduan dan prosedur keselamatan ICT di JPPM;

h) Melaporkan kepada CERT JPPM, CERT KDN seterusnya GCERT NACSA mengenai sebarang insiden keselamatan ICT yang berlaku di JPPM;

i) Membantu dalam membangunkan standard, garis panduan dan prosedur untuk aplikasi, sistem dan infrastruktur ICT di JPPM bagi mematuhi keperluan Dasar Keselamatan ICT KDN;

j) Mewujudkan program-program bagi meningkatkan pengetahuan, kesedaran dan pembudayaan mengenai teknologi dan mekanisme kawalan maklumat dan aset ICT, ancaman-ancaman siber serta peranan dan tanggungjawab pengguna dalam mengendalikan kemudahan ICT di JPPM;

k) Menyebarkan dan menyalurkan amaran awal terhadap ancaman-ancaman yang berpotensi menyebabkan kerosakan besar kepada aset ICT JPPM; dan

l) Mengurus keseluruhan program-program keselamatan ICT di JPPM.

m)

2.1.7 Bahagian Pengurusan Teknologi Maklumat (BPTM)

BPTM

BPTM adalah bahagian yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pelaksana dalam merumuskan rancangan dan strategi keselamatan ICT JPPM.

Mesyuarat BPTM dipengerusikan oleh Pengarah BPTM dan ahli-ahli terdiri daripada staf BPTM.

Bidang Kuasa:

a) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam JPPM yang mematuhi keperluan DKICT JPPM;
b) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;
c) Memastikan DKICT JPPM selaras dengan dasar-dasar ICT kerajaan semasa;
d) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; dan
e) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebaran insiden.

2.2 Pihak Ketiga

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).

2.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Bertujuan untuk memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal: Perkara yang perlu dipatuhi adalah seperti berikut:	CIO, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga

a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPPM;
b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;
c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;
d) Akses kepada aset ICT JPPM perlu berlandaskan kepada perjanjian kontrak;
e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai:
   i. Dasar Keselamatan ICT JPPM;
   ii. Surat Setuju Terima; dan
   iii. Hak Harta Intelek.
f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT JPPM sebagaimana **Lampiran 1**, dan Borang Perakuan Akta Rahsia Rasmi.
g) Melengkapkan proses tapisan keselamatan menggunakan Borang Tapisan Keselamatan Kasar atau Sistem e-Vetting.

2.2.2 Keselamatan Maklumat dalam Pengurusan Projek

Bertujuan untuk memastikan setiap pengurusan projek (tanpa mengira jenis projek) yang dilaksanakan oleh JPPM mengambilkira aspek keselamatan maklumat secara holistik. ICTSO

ICTSO adalah bertanggungjawab untuk :

a) Menjadikan objektif keselamatan maklumat sebahagian daripada objektif projek;
b) Memastikan pengurusan projek mematuhi manual keselamatan dan polisi DKICT dalam setiap aktiviti pengurusan projek; dan
c) Memastikan semua pihak yang terlibat dalam sesuatu projek maklum tentang arahan berkaitan keselamatan maklumat dan mereka diikat dengan perjanjian (seperti Akta Rahsia Rasmi).

2.2.3 Polisi Keselamatan Maklumat berkaitan Hubungan Pembekal

Seksyen ini menjelaskan keperluan untuk mendokumentasikan strategi mitigasi risiko keselamatan maklumat bilamana pembekal dibenarkan untuk akses kepada aset ICT JPPM. ICTSO

ICTSO adalah bertanggungjawab untuk :

a) Mengenalpasti dan mendokumenkan jenis-jenis pembekal (seperti khidmat servis IT, pembekal infrastruktur IT, logstik, kewangan dsb.);
b) Mengenalpasti jenis aset maklumat yang dibenarkan untuk diakses oleh pembekal serta melakukan pemantauan dan pengawalan terhadap aset tersebut secara berterusan;
c) Memberi pendedahan terhadap polisi, proses, dan prosedur berkaitan keselamatan maklumat.
d) Mewujudkan mekanisma/proses pengurusan pembekal dengan mengambil kira aspek keselamatan maklumat sebagai teras;
e) Memastikan pemantauan berterusan dilakukan terhadap semua pembekal dengan melaksanakan pengukuran prestasi dan pematuhan terhadap garis panduan keselamatan maklumat;
f) Mewujudkan kontrak rasmi bersama pembekal yang dapat menjamin keselamatan maklumat JPPM disamping segala urusan bersama pembekal hendaklah dilaksanakan secara rasmi; dan
g) Mewujudkan perjanjian yang jelas agar pihak pembekal memastikan keselamatan maklumat yang digunakan terjamin sepanjang akses dibenarkan dan seterusnya memulangkan kembali semua aset maklumat sekiranya kontrak mereka tamat atau ditamatkan.

2.2.4 Rangkaian Pembekal ICT

Seksyen ini menjelaskan kandungan perjanjian bersama pembekal yang perlu diwujudkan bagi memastikan risiko keselamatan maklumat berkaitan rangkaian pembekal khidmat ICT dan produk diambil kira. ICTSO

ICTSO adalah bertanggungjawab untuk :

a) Mengenalpasti keperluan keselamatan maklumat khusus berkaitan dengan perolehan rangkaian pembekal servis ICT dan produk sebagai tambahan kepada keperluan umum keselamatan maklumat berkaitan hubungan pembekal yang telah dikenal pasti;
b) Memastikan rangkaian pembekal yang terlibat dalam menyediakan khidmat servis ICT berkongsi hal berkaitan keselamatan maklumat (polisi, prosedur, proses) kepada setiap aras pembekal termasuk sub-pembekal atau sub-sub-pembekal;
c) Melaksanakan proses pemantauan rangkaian pembekal servis ICT dan produk dengan kaedah yang berkesan bagi menjamin keperluan keselamatan maklumat sentiasa dipatuhi;
d) Mendapatkan jaminan bahawa komponen produk yang kritikal boleh berfungsi mengikut spesifikasi dan dikesan sumbernya dari rangkaian pembekal yang pelbagai;
e) Mewujudkan peraturan yang khusus bagi mengawal perkongsian maklumat dikalangan rangkaian pembekal;
f) Mewujudkan mekanisma khusus untuk mengurus rangkaian pembekal khidmat servis ICT dan produk bagi memastikan keselamatan maklumat terjamin. Mekanisma yang diwujudkan wajar mampu untuk mengurus risiko sekiranya komponen produk yang dibekalkan tidak lagi boleh dibekalkan kerana perubahan trend dan teknologi yang berlaku.

BIDANG 03 PENGURUSAN ASET

3.1 Akauntabiliti Aset

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JPPM

3.1.1 Inventori Aset ICT

Bertujuan untuk memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

Semua

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini;
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 JPPM;
d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan
e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

.

3.2 Pengelasan dan Pengendalian Maklumat

Objektif:

Memastikan setiap maklumat atau asset ICT diberikan tahap perlindungan yang bersesuaian.

3.2.1 Pengelasan Maklumat

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad.	Semua

3.2.2 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:	Semua

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;
d) Menjaga kerahsiaan kata laluan;
e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

BIDANG 04 KESELAMATAN SUMBER MANUSIA

4.1 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan JPPM, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga JPPM hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

4.1.1 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: Semua

a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan JPPM serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan JPPM serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan
c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

4.1.2 Dalam Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: Semua

a) Memastikan pegawai dan kakitangan JPPM serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh JPPM;
b) Memastikan kesedaran mengenai pengurusan keselamatan aset ICT diberi kepada pengguna JPPM secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;
c) Memastikan adanya proses tindakan disiplin dan/atau undang- undang ke atas pegawai dan kakitangan JPPM serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh JPPM; dan
d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Sumber Manusia dan Khidmat Pengurusan (BSMKP), JPPM.

4.1.3 Bertukar atau Tamat Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: Semua

a) Memastikan semua aset ICT dikembalikan kepada JPPM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh JPPM dan/atau terma perkhidmatan.

BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.1 Keselamatan Kawasan

Objektif:

Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan

5.1.1 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. — CIO dan ICTSO

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a) Kawalan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi asset dan hasil penilaian risiko;
b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
c) Memasang alat penggera atau kamera;
d) Menghadkan jalan keluar masuk;
e) Mewujudkan perkhidmatan kawalan keselamatan;
f) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
g) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan yang disediakan; dan
h) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana.

5.1.2 Kawalan Masuk Fizikal

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:	Semua

a) Setiap pengguna JPPM hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;
b) Semua pas keselamatan hendaklah diserahkan balik kepada BSMKP, JPPM apabila pengguna berhenti atau bersara; dan
c) Kehilangan pas mestilah dilaporkan dengan segera.

5.1.3 Kawasan Larangan

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut.	Semua

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a) Akses kepada kawasan larangan hanyalah kepada pegawai- pegawai yang dibenarkan sahaja; dan
b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.

5.2 Keselamatan Peralatan

Objektif:

Melindungi peralatan ICT JPPM dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

5.2.1 Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;
b) Pengguna bertanggungjawab sepenuhnya ke atas komputer, komputer riba, dan *tablet* masing-masing dan tidak dibenarkan membuat sebarang pengubahsuaian komponen dan konfigurasi yang telah ditetapkan;
c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan ICT yang telah ditetapkan;
d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa lesen;
e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;
f) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;
g) Peralatan-peralatan kritikal seperti pelayan perlu disokong oleh *Uninterruptable Power Supply* (UPS);
h) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;
i) Semua peralatan ICT yang digunakan secara berterusan

mestilah diletakkan di kawasan yang berhawa dingin atau mempunyai pengudaraan (*air ventilation*) yang sesuai;

j) Peralatan ICT yang hendak dibawa keluar dari premis JPPM oleh pihak ketiga, perlulah mendapat kelulusan pegawai yang bertanggungjawab dan direkodkan bagi tujuan pemantauan;

k) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

l) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran pegawai yang bertanggungjawab;

m) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada pegawai yang bertanggungjawab untuk dibaik pulih;

n) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

o) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan;

p) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi ururan rasmi sahaja;

q) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; dan

r) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.

5.2.2 Media Storan

Keselamatan media storan perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat.	Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;
c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;
e) Akses dan pergerakan media storan hendaklah direkodkan;
f) Peralatan *backup* hendaklah diletakkan di tempat yang terkawal;
g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;
h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan
i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.

5.2.3 Media Tandatangan Digital

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;
b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan
c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.

5.2.4 Media Perisian dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Hanya perisian yang berlesen dan diperakui sahaja dibenarkan bagi kegunaan JPPM;
b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengarah BPTM;
c) 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
d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

5.2.5 Penyelenggaraan Peralatan ICT

Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Semua peralatan ICT yang diselenggara hendaklah mematuhi prosedur penyelenggaraan yang ditetapkan oleh JPPM;
b) Memastikan peralatan ICT hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;
c) Menyemak dan menguji semua peralatan ICT sebelum dan selepas proses penyelenggaraan; dan
d) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

5.2.6 Peralatan ICT di Luar Premis

Peralatan ICT yang dibawa keluar dari premis JPPM adalah terdedah kepada pelbagai risiko. Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Peralatan ICT perlu dilindungi dan dikawal sepanjang masa; dan
b) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

5.2.7 Pelupusan Peralatan ICT

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan JPPM. a) Menghapuskan semua kandungan khususnya maklumat rahsia rasmi terlebih dahulu sama ada melalui *shredding, grinding, degauzing* atau pembakaran sebelum pelupusan; dan b) Merujuk kepada 1 Pekeliling Perbendaharaan (1PP) – Tatacara Pengurusan Aset Alih Kerajaan: Pelupusan yang terkini.	Semua, Pegawai Aset dan BPTM

5.3 Keselamatan Persekitaran

Objektif:

Melindungi aset ICT JPPM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

5.3.1 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Kementerian Dalam Negeri

Semua

Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi:

a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;
b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;
c) Peralatan perlindungan 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;
g) Semua peralatan perlindungan hendaklah disemak dan

diuji sekurang-kurangnya satu (1) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan

h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.

5.3.2 Bekalan Kuasa

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. — BPTM dan ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;

b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*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.

5.3.3 Kabel

Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi.	BPTM dan ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan
d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.

5.3.4 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

a) Setiap pengguna hendaklah memahami dan mematuhi prosedur kecemasan JPPM
b) ; dan
c) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan yang dilantik.

5.4 Keselamatan Dokumen

Objektif:

Melindungi maklumat JPPM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

5.4.1 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;
b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;
c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;
d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan
e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.

BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI

6.1 Pengurusan Prosedur Operasi

Objektif:

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

6.1.1 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal;
b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan
c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

6.1.2 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Pengubahsuaian yang melibatkan peralatan ICT, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;
b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus

dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan asset ICT berkenaan;

c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan

d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

6.1.3 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: ICTSO

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 diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan

c) Peralatan ICT yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari peralatan ICT yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif:

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

6.2.1 Perkhidmatan Penyampaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;
b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan
c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

6.3 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

6.3.1 Perancangan Kapasiti

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. 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.	Pentadbir Sistem ICT dan ICTSO

6.3.2 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi criteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT dan ICTSO

6.4 Perisian Berbahaya

Objektif:

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *Trojan* dan sebagainya.

6.4.1 Perlindungan dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;
b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;
c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;
d) Mengemas kini anti virus dengan *pattern* antivirus yang terkini;
e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;
h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan
i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

6.4.2 Perlindungan dari *Mobile Code*

Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua

6.5 *Housekeeping*

Objektif:

Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

6.5.1 *Backup*

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. — Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat;
c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;
d) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan
e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat..

6.6 Pengurusan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

6.6.1 Kawalan Infrastruktur Rangkaian

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. BPTM

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;
b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;
c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;
e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir ICT;
f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JPPM;
g) Semua perisian *sniffer atau network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;
h) Memasang perisian *Intrusion Prevention System* (IPS) bagi. mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JPPM;

i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;
j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan JPPM adalah tidak dibenarkan;
k) Semua pengguna hanya dibenarkan menggunakan rangkaian JPPM sahaja dan penggunaan modem adalah dilarang sama sekali; dan
l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.

6.7 Pengurusan Media

Objektif:

Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

6.7.1 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua

6.7.2 Prosedur Pengendalian Media

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang	Semua

tidak dibenarkan;

e) Menyimpan semua media di tempat yang selamat; dan
f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.

6.7.3 Keselamatan Sistem Dokumentasi

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: Semua

a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;
b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan
c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.

6.8 Pengurusan Pertukaran Maklumat

Objektif:

Memastikan keselamatan pertukaran maklumat dan perisian antara JPPM dan agensi luar terjamin.

6.8.1 Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;
b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara JPPM dengan agensi luar;

c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari JPPM; dan
d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.

6.8.2 Pengurusan Mel Elektronik (E-mel)

Penggunaan e-mel di JPPM hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana- mana undang-undang bertulis yang berkuat kuasa. Semua

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:

a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh JPPM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh JPPM;
c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;
d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;
e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi lima belas megabait (15 Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;
f) Pengguna hendaklah mengelak dari membuka e-mel

daripada penghantar yang tidak diketahui atau diragui;

g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;

i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan

m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbo*x* masing-masing.

6.8.3 *Bring Your Own Device* (BYOD)

Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD seperti berikut: Semua

a) Semua peringkat maklumat rasmi kerajaan adalah hak milik kerajaan; dan
b) Sebarang bahan rasmi yang dimuat naik/edar/kongsi hendaklah mendapat kebenaran Ketua Jabatan.

Pengguna BYOD adalah DILARANG daripada melakukan perkara berikut:

a) Menggunakan peranti milik sendiri untuk mengakses, menyimpan dan menyebarkan maklumat Rasmi dan Terperingkat kepada pihak yang tidak dibenarkan;
b) Penggunaan peranti milik sendiri untuk tujuan peribadi yang boleh menggangu produktiviti kerja;
c) Menjadikan peranti milik sendiri sebagai medium sandaran (backup) bagi maklumat Rasmi;
d) Merakam komunikasi dan dokumen rasmi untuk tujuan peribadi; dan
e) Menjadikan peranti milik sendiri sebagai *access point* kepada aset ICT jabatan untuk capaian ke *Internet*.

Pengguna BYOD perlu memastikan peranti yang digunakan mempunyai kawalan keselamatan seperti berikut:

a) Menetapkan mekanisme kawalan akses bagi peranti milik sendiri dan akan mengunci secara automatik apabila tidak digunakan;
b) Melaksanakan penyulitan dan/atau perlindungan ke atas folder yang mempunyai maklumat rasmi Kerajaan yang disimpan di dalam peranti milik sendiri;
c) Memuat turun aplikasi daripada sumber yang sah; dan
   Memastikan peranti milik sendiri mempunyai ciri-ciri keselamatan standard.

Pengguna BYOD adalah tertakluk kepada perkara-perkara seperti berikut:

a) Kakitangan adalah bertanggungjawab menggunakan peranti milik sendiri secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/dasar yang berkuatkuasa;
b) Kakitangan bertanggungjawab memadamkan segala maklumat yang berkaitan dengan urusan rasmi jabatan sekiranya bertukar/ditamatkan perkhidmatan/ bersara ATAU sewaktu dihantar ke pusat servis untuk penyelenggaraan;
c) Kakitangan adalah bertanggungjawab dan boleh dikenakan tindakan tatatertib sekiranya didapati menyalahgunakan peranti milik sendiri yang menyebabkan kehilangan/kerosakan/pendedahan maklumat rasmi Kerajaan;
d) JPPM tidak bertanggungjawab atas kehilangan atau kerosakan data peranti milik sendiri yang digunakan untuk tujuan urusan rasmi jabatan; dan
e) Peranti mudah alih yang merupakan aset JPPM tidak tertakluk kepada dasar ini. Pengguna tersebut masih tertakluk kepada langkah-langkah perlindungan keselamatan yang berkuatkuasa.

6.9 Perkhidmatan E-Dagang (*Electronic Commerce Services)*

Objektif:

Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

6.9.1 E-Dagang

Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan *Internet*. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua

6.9.2 Maklumat Umum

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua

6.10 Pemantauan

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

6.10.1 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: ICTSO

a) Sebarang percubaan pencerobohan kepada sistem ICT JPPM;
b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); dan
c) Pengubahsuaian ciri-ciriperalatan, perisian atau mana-mana komponen sesebuah sistem tanpa 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 jalur lebar (*bandwidth*) rangkaian;
g) Aktiviti penyalahgunaan akaun e-mel; dan
h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.

6.10.2 Jejak Audit

Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.

Pentadbir Sistem ICT

Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

a) Rekod setiap aktiviti transaksi;
b) Maklumat jejak audit sekurang-kurangnya mengandungi identiti pengguna, perubahan maklumat, tarikh aktiviti dan masa aktiviti.
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 Arahan Teknologi Maklumat dan Akta Arkib Negara.

Pentadbir Sistem ICT 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 dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

6.10.3 Sistem Log

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: — Pentadbir Sistem ICT

a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan
c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO .

6.10.4 Pemantauan Log

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — BPTM dan Pentadbir Sistem ICT

a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;
b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala;
c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;
d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;
e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan
f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JPPM atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

BIDANG 07 KAWALAN CAPAIAN

7.1 Dasar Kawalan Capaian

Objektif:

Mengawal capaian ke atas maklumat.

7.1.1 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.	BPTM dan ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;
b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan
d) Kawalan ke atas kemudahan pemprosesan maklumat.

7.2 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT JPPM.

7.2.1 Akaun Pengguna

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.

Semua dan Pentadbir Sistem ICT

Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:

a) Akaun yang diperuntukkan oleh JPPM sahaja boleh digunakan;
b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;
c) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan JPPM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan
e) Pentadbir Sistem ICT boleh membeku, menghadkan atau menamatkan akaun pengguna atas sebab-sebab berikut:
    i. Pengguna bertukar jawatan, tanggungjawab dan/atau dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib; dan
    ii. Pengguna bertukar, berpindah agensi, bersara dan/atau tamat perkhidmatan.

7.2.2 Hak Capaian

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT

7.2.3 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 JPPM seperti berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah dimasukkan dalam bentuk yang tidak boleh dilihat, tidak dipaparkan dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; h) Kata laluan hendaklah ditukar selepas enam (6) bulan atau selepas tempoh masa yang bersesuaian; dan i) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	Semua dan Pentadbir Sistem ICT

7.2.4 *Clear Desk* dan *Clear Screen*

Semua

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;
b) Menyimpan bahan dan maklumat terperingkat yang sensitif di dalam laci atau kabinet fail yang berkunci; dan
c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.

7.3 Kawalan Capaian Rangkaian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

7.3.1 Keperluan Kawalan Capaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: — Pentadbir Sistem ICT dan ICTSO

a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian JPPM, rangkaian agensi lain dan rangkaian awam;
b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan
c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

7.3.2 Capaian Internet

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Pentadbir Rangkaian

a) Penggunaan Internet di JPPM hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian JPPM;
b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;
c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti

(*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;

d) Laman yang dilayari hendaklah hanya yang berkaitan dengan semua bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/ pegawai yang diberi kuasa; — Semua

e) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

f) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet;

g) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

h) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh JPPM;

i) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

j) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:

   i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan

   ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah

7.4 Kawalan Capaian Sistem Pengoperasian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

7.4.1 Capaian Sistem Pengoperasian

Pentadbir Sistem ICT dan ICTSO

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:

a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan
b) Merekodkan capaian yang berjaya dan gagal.

Kaedah-kaedah yang digunakan hendaklah JPPM menyokong perkara-perkara berikut:

a) Mengesahkan pengguna yang dibenarkan;
b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan
c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;
b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;
c) Menghadkan dan mengawal penggunaan program; dan
d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

7.4.2 Kad Pintar

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

a) Penggunaan kad pintar hendaklah digunakan bagi capaian sistem yang dikhususkan;
b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;
c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; dan
d) Sebarang kehilangan dan kerosakan kad pintar perlu dimaklumkan kepada pihak yang berkaitan.

7.5 Kawalan Capaian Pangkalan Data

Seksyen ini bertujuan untuk memastikan capaian ke atas pangkalan data dan data dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong pengesahan pengguna, mewujudkan jejak audit ke atas semua capaian, menjana amaran (alert), pengesahan capaian dan penyimpanan data.

Semua

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada perkara berikut:

a) Capaian ke atas pangkalan data hendaklah dikawal.
b) Penggunaan perisian yang membolehkan capaian terus ke pangkalan data secara pihak ketiga sama ada melalui perisian web (contoh: phpmyadmin) atau sebagainya adalah tidak dibenarkan
c) Mewujudkan pengenalan diri (ID) yang unik bagi setiap pengguna dan hanya digunakan untuk pengguna berkenaan sahaja.
d) Aplikasi yang perlu mengakses ke pangkalan data perlu menggunakan pengenalan diri yang berbeza daripada pengenalan diri pembangun aplikasi dan pentadbir pangkalan data.

7.6 Kawalan Capaian Aplikasi dan Maklumat

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.

7.6.1 Capaian Aplikasi dan Maklumat

Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.	Pentadbir Sistem ICT dan ICTSO

Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara- perkara berikut hendaklah dipatuhi:

a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;
b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);
c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; dan
d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.

7.7 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif:

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

7.7.1 Peralatan Mudah Alih

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Peralatan mudah alih hendaklah sentiasa dikunci dengan menggunakan *cable lock;* dan
b) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

7.7.2 Kerja Jarak Jauh

Perkara yang perlu dipatuhi adalah seperti berikut: Semua

a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.

BIDANG 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

8.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:

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

8.1.1 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;
b) Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat;
c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan
d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.

8.2 Kawalan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

8.2.1 Enkripsi (*Encryption)*

Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua

8.2.2 Tandatangan Digital (*Digital Signature)*

Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik..	Pengguna berkaitan

8.2.3 Pengurusan Infrastruktur Kunci Awam (PKI)

Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut	Semua

8.3 Keselamatan Fail Sistem

Objektif:

Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

8.3.1 Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Pemilik Sistem dan Pentadbir Sistem ICT

a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;
b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;
c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;
d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan
e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

8.4 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

8.4.1 Prosedur Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Pemilik Sistem dan Pentadbir Sistem ICT

a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;
b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian dan pangkalan data untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan;
c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;
d) Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan;
e) Menghalang sebarang peluang untuk membocorkan maklumat;dan
f) Kawalan yang bersesuaian dan log audit perlu di reka bentuk ke dalam sistem aplikasi. Ini termasuklah pengesahan data yang dimasukkan, data yang dihasilkan, pemprosesan dalaman, pengesahan dan integriti mesej dan sebagainya. Ukuran keselamatan mesti dititik beratkan semasa membangunkan aplikasi baru atau mengemas kini / menambah baik aplikasi sedia ada

8.4.2 Pembangunan Perisian Secara *Outsource*

Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik JPPM.	BPTM dan Pentadbir Sistem ICT

8.4.3 Dasar Keselamatan dalam Pembangunan Sistem

Seksyen ini bertujuan memastikan keselamatan maklumat direkabentuk dan dilaksanakan di dalam setiap kitaran pembangunan sistem.	ICTSO dan Pentadbir Sistem ICT

Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan di dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut:

a) Keselamatan repositori;
b) Keperluan pengetahuan keselamatan dalam pembangunan perisian; dan
c) Kod aturcara perlu selamat dan bebas daripada sebarang ancaman pencerobohan.

8.4.4 Prinsip Kejuruteraan Keselamatan Sistem

a) Keselamatan perlu diambil kira dalam semua peringkat pembangunan sistem. b) Prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa bagi memastikan keberkesanan kepada keselamatan maklumat.	ICTSO dan Pentadbir Sistem ICT

8.4.5 Keselamatan Persekitaran Pembangunan Sistem

ICTSO dan Pentadbir Sistem perlu memastikan:	ICTSO dan Pentadbir Sistem ICT
a) Keselamatan persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem (*development lifecycle*).	

8.4.6 Pengujian Keselamatan Sistem

ICTSO dan Pentadbir Sistem perlu memastikan:	ICTSO dan Pentadbir Sistem
b) Pengujian fungsi keselamatan perlu dijalankan semasa proses pembangunan samada bagi pembangunan secara dalaman (in-house) atau pembangunan melalui sumber luar (outsource).	

8.5 Kawalan Teknikal Keterdedahan (*Vulnerability)*

Objektif:

Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

8.5.1 Kawalan dari Ancaman Teknikal

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan	Pentadbir Sistem ICT
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	
a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;	

b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan
c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

8.5.2 Sekatan dalam Instalasi Perisian

Seksyen ini menjelaskan peraturan berhubung instalasi perisian yang perlu diwujud dan dilaksanakan. — ICTSO

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

a) Prinsip keutamaan rendah wajar diadaptasi dalam peraturan instalasi perisian. Jika sesuatu keizinan diberikan, kemampuan pengguna perlu dipastikan untuk melaksanakan proses instalasi.
b) Semua pengguna tidak dibenarkan memindah turun, membuat instalasi dan mengguna perisian yang boleh mendatangkan kemudaratan dan kerosakan kepada komputer dan rangkaian misalnya perisian P2P (peer to peer) Internet seperti Bittorrent, Utorrent, Aries, Deluge, Vuze dan sebagainya — Semua
c) Semua pengguna tidak dibenarkan menyebar sebarang perisian berlesen secara tidak sah. JPPM tidak akan bertanggungjawab ke atas sebarang kesalahan yang dilakukan oleh pengguna.

BIDANG 09 PENGURUSAN INSIDEN KESELAMATAN

9.1 Menangani Insiden Keselamatan ICT

Objektif:

Memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan serta meminimumkan kesan insiden keselamatan ICT.

9.1.1 Prosedur Pengurusan Insiden

Prosedur pengurusan insiden perlu diwujudkan dan didokumenkan. — ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan indentiti dan pengubahsuaian perisian tanpa kebenaran;
b) Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;
c) Menyimpan *audit trail* dan memelihara bahan bukti;dan
d) Menyediakan pelan tindakan pemulihan segera.

9.1.2 Pelaporan Insiden

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO / Pegawai yang berkaitan dengan kadar segera. — Semua

Insiden keselamatan ICT adalah termasuk yang berikut:

a) Mendapati maklumat hilang, terdedah kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang;
b) Mendapati sistem maklumat yang digunakan tanpa kebenaran atau disyaki sedemikian;

c) Mendapati kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
d) Mendapati kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
e) Mendapati berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini

9.1.3 Penilaian dan Keputusan terhadap Insiden Keselamatan ICT

Insiden keselamatan ICT perlu dinilai dan keputusan perlu dibuat jika pasti insiden tersebut boleh diklasifikasikan sebagai insiden keselamatan maklumat. — ICTSO, CERT

a) Penilaian perlu dibuat berasaskan skim klasifikasi insiden yang dipersetujui;
b) Insiden perlu disusun mengikut kepentingan dan implikasi kepada JPPM;
c) Hasil daripada penilaian yang dibuat boleh dipanjangkan kepada CERT supaya pengesahan atau penilaian semula dapat dilakukan;
d) Hasil daripada penilaian juga perlu direkodkan dengan terperinci untuk rujukan masa depan dan penentusahan.

9.1.4 Tindakbalas terhadap Insiden Keselamatan ICT

Insiden keselamatan maklumat perlu diberi tindakbalas sewajarnya oleh pihak yang bertanggungjawab mengikut prosidur yang berkaitan. Matlamat utama tindakbalas terhadap insiden keselamatan ICT adalah untuk mengembalikan tahap keselamatan ke paras normal dan seterusnya melaksanakan langkah-langkah perlu pemulihan.

ICTSO, CERT

Pasukan tindakbalas wajar melaksanakan perkara berikut:

e) Mengumpul bahan bukti secepat yang mungkin selepas kejadian;
f) Melaksanakan forensik keselamatan maklumat;
g) Insiden dimaklumkan kepada pihak yang berkaitan atau perlu tahu;
h) Semua aktiviti dalam memberi tindakbalas direkod secara sistematik untuk analisis selanjutnya;
i) Mengendalikan dengan efektif kelemahan-kelemahan keselamatan maklumat yang diketahui menjadi penyebab atau penyumbang kepada sesuatu insiden berlaku;
j) Selepas sesuatu insiden ditangani dengan sempurna, penutupan kes secara rasmi perlu dilakukan dengan rekod;
k) Analisa pasca insiden wajar dilakukan untuk mengenalpasti punca insiden;

BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

10.1 Dasar Kesinambungan Perkhidmatan

Objektif:

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

10.1.1 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan (*Business Continuity Management* – BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan.

CIO, ICTSO, Pasukan Pemulihan Bencana JPPM

Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Perkara-perkara berikut perlu diberi perhatian:

a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;
c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
d) Mendokumentasikan proses dan prosedur yang telah dipersetujui;
e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
f) Membuat *backup*; dan

g) Menguji dan mengkaji semula pelan sekurang-kurangnya setahun sekali.

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b) Senarai personel JPPM dan pihak pembekal berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel) ;
c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
e) Perjanjian dengan pihak pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan yang berkaitan.

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan sekiranya perlu.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.
JPPM hendaklah memastikan salinan pelan BCM sentiasa dikemaskini dan dilindungi seperti di lokasi utama.

10.1.2 Kebolehsediaan Fasiliti Pemprosesan Maklumat

Untuk memastikan kebolehsediaan fasiliti pemprosesan maklumat ditahap yang tinggi, kaedah pemprosesan bertindan (lebih dari satu lokasi/platform pemprosesan) perlu diwujudkan. CIO/ ICTSO

Untuk tujuan itu, perkara berikut wajar diberi tumpuan:

a) JPPM perlu mengenalpasti keperluan kebolehsediaan sistem maklumat (memahami sejauh mana kritikalnya kebolehsediaan sesuatu sistem maklumat);
b) Jika kebolehsediaan sistem maklumat tidak dapat dipastikan dengan satu lokasi pemprosesan, maka fasiliti pemprosesan bertindan perlu dipertimbangkan;
c) Fasiliti pemprosesan bertindan perlu diuji bagi memastikan kesiapsediaan menjalankan operasi apabila pemprosesan utama gagal berfungsi;
d) Kewujudan pemprosesan bertindan boleh membawa risiko kepada kewibawaan dan kerahsiaan maklumat dan sistem maklumat. Hal ini perlu diambil kira semasa sesuatu sistem maklumat itu direkabentuk.

BIDANG 11 PEMATUHAN

11.1 Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT JPPM.

11.1.1 Pematuhan Dasar

Setiap pengguna di JPPM hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT JPPM dan undang-undang atau peraturan- peraturan lain yang berkaitan yang berkuat kuasa	Semua
Semua aset ICT di JPPM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	
Sebarang penggunaan aset ICT JPPM selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalangunaan sumber JPPM.	

11.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.	ICTSO
Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.	

11.1.3 Pematuhan Keperluan Audit

Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	Semua

11.1.4 Keperluan Perundangan

Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di JPPM adalah seperti di Lampiran 2.	Semua

11.1.5 Pelanggaran Dasar

Sebarang pelanggaran dasar dan peraturan oleh pengguna akan dikenakan tindakan berdasarkan kepada jenis pelanggaran dan keadaan semasa pelanggaran. Sebarang aduan tentang pelanggaran Dasar hendaklah dibuat secara bertulis kepada CIO. CIO boleh melantik Jawatankuasa Penyiasat untuk meneliti laporan dan boleh membuat keputusan sama ada siasatan terperinci perlu dilaksanakan. Tindakan atau penalti yang boleh dikenakan oleh CIO adalah penggantungan penggunaan kemudahan ICT. Lain-lain tindakan atau penalti boleh diambil dengan mengikut prosedur yang ditetapkan.	Semua

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk peralatan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan 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 peralatan atau perisian atau kombinasi kedua-duanya
Forgery	Pemalsuan dan penyamaran identity yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.

Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain
ICT	*Information and Comminication Technology* (Komunikasi dan Teknologi Maklumat)
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem maklumat.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan,
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan. Perisian atau peralatanyang 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.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan. Peralatan keselamatan computer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code.* Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network.* Rangkaian Kawasan Setempat yang menghubungkan komputer.

Logout	Keluar daripada sesuatu sistem atau aplikasi komputer
Malicious Code	atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya
MODEM	MOdulator DEModulator. Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi- fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, capaian Internet
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan computer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika

	ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
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
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT
JABATAN PENDAFTARAN PERTUBUHAN MALAYSIA

Nama : .....
No. Kad Pengenalan : .....
Jawatan : .....
Bahagian/JPPM Negeri : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT JPPM; atau
2. Saya telah mengikuti Taklimat Dasar Keselamatan ICT JPPM; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....
(Tandatangan)

Tarikh : .....

Disahkan Oleh:	**Diperakukan Oleh:**
Pegawai Keselamatan ICT (ICTSO) / CIO JPPM	**Ketua Pegawai Maklumat (CIO) / Ketua Pengarah JPPM**
.....	.....
( )	( )
Tarikh:	Tarikh: .....

Lampiran 2

SENARAI PERUNDANGAN DAN PERATURAN

1) Akta Rahsia Rasmi 1972;
2) Akta Tandatangan Digital 1997;
3) Akta Jenayah Komputer 1997;
4) Akta Hak Cipta (Pindaan) 2012;
5) Akta Komunikasi dan Multimedia 1998;
6) Akta Pertubuhan 1966;
7) Akta Pencegahan Dan Pengawalan Penyakit Berjangkit 1988;
8) Arahan Keselamatan;
9) Arahan Pendaftar Pertubuhan;
10) Arahan Teknologi Maklumat 2007;
11) Perintah-Perintah Am;
12) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi- Agensi Kerajaan yang bertarikh 20 Oktober 2006;
13) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
14) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
15) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.

16) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
17) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
18) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
19) Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
20) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
21) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
22) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
23) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
24) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
25) 1 Pekeliling Perbendaharaan (1PP) – Tatacara Pengurusan Aset Alih Kerajaan;
26) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
27) Peraturan-Peraturan Pencegahan Dan Pengawalan Penyakit Berjangkit (Pengkompaunan Kesalahan-Kesalahan) (Pindaan) (No.7) 2020;

28) Peraturan-Peraturan Pencegahan Dan Pengawalan Penyakit Berjangkit (Langkah-Langkah Di Dalam Kawasan Tempatan Jangkitan) (No.7) 2020.