JABATAN
PENDAFTARAN
PERTUBUHAN
MALAYSIA

POLISI KESELAMATAN SIBER (PKS)

VERSI 1.0 | 6 OKTOBER 2022

Polisi Keselamatan Siber Jabatan Pendaftaran Pertubuhan Malaysia (JPPM) adalah terpakai untuk Ibu Pejabat JPPM serta JPPM Negeri seluruhnya.

REKOD PINDAAN

TARIKH	VERSI	BAB/MUKA SURAT	BUTIRAN PINDAAN
6 Oktober 2022	1.0	Keseluruhan Dokumen	Keluaran pertama diluluskan dalam Mesyuarat JPICT JPPM Bil. 2/2022 pada 6 Oktober 2022.

ISI KANDUNGAN

GLOSARI	
Alamat IP	Alamat Protokol Internet/*Internet Protocol* (IP) adalah suatu nombor unik yang digunakan oleh peranti sebagai pengenalan dan untuk berkomunikasi antara satu sama lain di dalam satu rangkaian komputer yang menggunakan piawaian Protokol Internet (IP).
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	Komponen ICT termasuk peralatan, perisian, sistem aplikasi, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur lebar. Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
Beyond Economic Repair BER	Aset ICT yang tidak lagi optimum dari segi komersil untuk dibaik pulih.
CDO	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service (DoS)	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah pemprosesan suatu utusan oleh pengirimnya supaya tidak difahami oleh orang lain kecuali penerima yang sah.
End of Life (EOL)	Aset ICT atau komponen berkaitan yang telah tamat kitaran hidup.
End of Support (EOS)	Aset ICT atau komponen berkaitan tidak lagi diberi sokongan teknikal oleh pembuat aset tersebut.
Firewall	Sistem yang direka bentuk untuk menghalang akses 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 termasuklah penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*) dan penipuan (*hoaxes*).
CSIRT	*Cyber Security Incident Response Team* atau Pasukan Tindak Balas Insiden Keselamatan Siber. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan siber 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 dilantik oleh Jabatan, bertanggungjawab menyelaras dan melaksanakan perkara-perkara yang berkaitan dengan keselamatan ICT di Jabatan masing-masing.
Internet	Sistem rangkaian seluruh dunia di mana pengguna boleh membuat akses maklumat daripada 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 peralatan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau iaitu sama ada lebih

	bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan. Peralatan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicous code.* Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
Jejak audit/*audit trail*	Jejak atau bekas laluan yang ditinggalkan oleh sesuatu urusan atau transaksi apabila ia diproses. Jejak ini bermula daripada titik urusan dimulakan dan berakhir pada titik urusan tamat. Pada setiap tahap, rekod tertentu dirakamkan untuk membolehkan urusan jejak semula kepada sumber asalnya.
LAN	*Local Area Network.* Rangkaian kawasan setempat yang menghubungkan komputer.
Logout	Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Kod sumber atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Mobile code	Kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.
MODEM	Modulator DEModulator. Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan akses 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.
Pegawai Pengelas	Pegawai awam yang dilantik oleh Menteri, Menteri Besar atau Ketua Menteri sesuatu Negeri melalui suatu perakuan di bawah tandatangannya untuk mengelaskan apa-apa suratan rasmi,

	maklumat atau bahan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana-mana yang berkenaan.
Pelanggan	Pihak luaran, individu atau syarikat yang menerima perkhidmatan dari JPPM.
Pelanggaran keselamatan	Berlaku apabila akses kepada perkara rahsia rasmi menjadi terdedah kepada orang-orang yang tidak dibenarkan. Ia juga bermaksud apa-apa tindakan dalam persekitaran fizikal dan elektronik yang boleh megakibatkan ancaman terhadap keselamatan perlindungan. Dalam konteks ICT, pelanggaran keselamatan bermaksud musibah/*adverse event* yang berlaku ke atas sistem ICT.
Pelawat	Individu luar yang dibenarkan untuk melawat premis JPPM secara fizikal.
Pembekal	Pihak luaran yang membekalkan perkhidmatan kepada JPPM.
Pemilik Projek	Pasukan kerja yang dilantik bagi memastikan projek dilaksanakan secara sempurna.
Pentadbir ICT	Pegawai yang ditugaskan untuk mentadbir perkakasan dan perisian ICT termasuklah sistem pengoperasian, pangkalan data, aplikasi serta rangkaian.
Peralatan ICT	Merangkumi sistem komputer peribadi, terminal, alat-alat perpheral komputer, perkakasan dan rangkaian komunikasi, perisian komputer, sistem aplikasi, perkakasan storan, kemudahan peralatan sokongan, bekalan kuasa atau seumpamanya.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi.
Pihak Ketiga	Pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JPPM.
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

	(2) rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya akses Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Server/Pelayan Komputer.
Switches	Alat yang boleh menapis dan menghantar isyarat paket data di antara segmen rangkaian LAN.
Threat	Gangguan atau ancaman melalui pelbagai cara seperti e-mel dan surat yang bermotif peribadi serta atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa utama 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 interaktif yang membenarkan dua (2) atau lebih lokasi untuk berinteraksi melalui paparan video dua (2) hala dan audio secara serentak.
Virus	Kod yang bertujuan merosakkan data atau sistem aplikasi.
Warga JPPM	Kakitangan Kerajaan yang berkhidmat di Jabatan Pendaftaran Pertubuhan Malaysia sama ada berjawatan tetap, kontrak dan sambilan yang menggunakan perkhidmatan JPPM.
Wireless LAN	Rangkaian yang terhubung tanpa melalui kabel.

PENGENALAN

Polisi Keselamatan Siber (PKS) JPPM mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT). Dokumen ini juga menerangkan kepada semua warga JPPM dan pihak ketiga mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber dan di dalam aset ICT JPPM.

OBJEKTIF

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

Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi JPPM dengan memastikan semua aset ICT dilindungi.

Objektif utama PKS JPPM adalah seperti berikut:

a) menerangkan kepada semua pengguna merangkumi warga JPPM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JPPM mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber dan di dalam aset ICT JPPM;
b) memastikan keselamatan penyampaian perkhidmatan ICT JPPM di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;
c) memastikan kelancaran operasi JPPM dan mengurangkan risiko ancaman serangan siber;
d) melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari segi kesan kegagalan atau kelemahan merangkumi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
e) mencegah salah guna atau kecurian aset ICT Kerajaan;
f) meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan; dan
g) memperkemaskan pengurusan keselamatan siber JPPM.

PERNYATAAN DASAR

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

Keselamatan siber bermaksud keselamatan ke atas sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem ini secara fizikal atau maya, serta persekitaran fizikal sistem-sistem tersebut disimpan. Keselamatan siber berkait rapat dengan perlindungan ke atas aset ICT sama ada perkakasan, perisian, maklumat, manusia dan perkhidmatan. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a) melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari akses yang tidak dibenarkan;
b) menjamin setiap maklumat adalah tepat dan sempurna;
c) memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d) memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah.

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

a) **Kerahsiaan** – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
b) **Integriti** – Data dan maklumat hendaklah tepat, lengkap dan terkini serta hanya boleh diubah dengan cara yang dibenarkan;
c) **Tidak Boleh Disangkal** – Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal;
d) **Kesahihan** – Data dan maklumat hendaklah dijamin kesahihannya; dan
e) **Ketersediaan** – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain daripada itu, langkah-langkah ke arah menjamin keselamatan siber hendaklah bersandarkan kepada perkara-perkara berikut:

a) penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT;
b) ancaman yang wujud akibat daripada kelemahan tersebut;
c) risiko yang mungkin timbul; dan
d) langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Aset ICT JPPM terdiri daripada peralatan, perisian, perkhidmatan, data atau maklumat serta sumber manusia. PKS 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 serta dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan, ketepatan maklumat di samping untuk melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa, PKS JPPM ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang diwujudkan, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dibuat salinan keselamatan dan dimusnahkan melalui pewujudan dan penguatkuasaan sistem kawalan serta prosedur dalam pengendalian semua perkara-perkara berikut:

a) **Perkakasan**

   Semua aset ICT 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 *face recognition*;
iii. Perkhidmatan pihak ketiga seperti pembekal *Cloud Service Provider* (CSP) atau *Software-As-A-Service* (SaaS); dan
iv. 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 pelanggan, pangkalan data, fail-fail data, maklumat-maklumat arkib dan lain-lain;

e) **Sumber Manusia**

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

f) **Premis Komputer Dan Komunikasi**

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

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber 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 yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujudkan, 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 ke atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. memeriksa maklumat serta menentukan maklumat tersebut adalah tepat dan lengkap dari semasa ke semasa;
iii. menentukan maklumat yang sedia untuk digunakan;
iv. menjaga kerahsiaan kata laluan;

v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. memberi perhatian kepada maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d) **Pengasingan**

Tugas mewujudkan, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada akses yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat rahsia rasmi atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

e) **Pengauditan**

Pengauditan adalah tindakan pemeriksaan dan pengesahan untuk memastikan pengendalian berkaitan keselamatan atau keadaan yang mengancam keselamatan yang dikendalikan adalah tepat dan sahih. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f) **Pematuhan**

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

g) **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehakses. 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 mewujudkan mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN SIBER

JPPM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan kerentanan 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 maklumat atau siber secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan siber seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan siber berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan maklumat atau siber 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 maklumat atau siber selaras dengan keperluan semasa.

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 JPPM;
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 POLISI KESELAMATAN MAKLUMAT

0101 Polisi Keselamatan Maklumat

Objektif:

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

010101 Pelaksanaan Polisi

Polisi ini dilaksanakan oleh Ketua Pegawai Digital (CDO) dan disokong oleh Jawatankuasa Pemandu ICT.	CDO

010102 Penyebaran Polisi

Polisi ini perlu disebarkan kepada semua warga JPPM dan pihak ketiga termasuklah pembekal, pakar runding dan lain-lain.	CDO / ICTSO

010103 Penyelenggaraan Polisi

PKS 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 serta kepentingan sosial. Berikut adalah perkara-perkara yang perlu dilaksanakan bagi penyelenggaraan PKS JPPM: a) kenal pasti dan tentukan perubahan yang diperlukan; b) kemukakan cadangan pindaan dalam Mesyuarat	CDO / ICTSO

Jawatankuasa Pemandu ICT JPPM untuk kelulusan; dan

c) Polisi ini hendaklah dikaji semula sekurang-kurangnya dua (2) tahun sekali atau mengikut keperluan semasa.

010104 Pengecualian Polisi

PKS JPPM adalah terpakai kepada warga JPPM dan pihak ketiga serta tiada pengecualian diberikan.	Warga JPPM dan Pihak Ketiga

BIDANG 02 ORGANISASI KESELAMATAN MAKLUMAT

0201 Infrastruktur Keselamatan Organisasi

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas serta teratur dalam mencapai objektif PKS JPPM.

020101 Struktur Organisasi

Jawatankuasa Pemandu ICT JPPM, JPPM CSIRT dan Jawatankuasa Kajian Semula Pengurusan ISMS JPPM adalah bertanggungjawab terhadap pengurusan keselamatan siber JPPM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) komitmen pengurusan atasan ke atas keselamatan siber hendaklah dilaksanakan dengan aktif dan telus; b) aktiviti pengurusan keselamatan siber diselaraskan oleh Ketua Pengarah, CDO dan Pegawai Keselamatan ICT (ICTSO) berdasarkan peranan masing-masing; c) menetapkan tanggungjawab yang jelas bagi semua warga JPPM dalam pengurusan keselamatan siber; d) keperluan untuk pengurusan kerahsiaan maklumat hendaklah dikenal pasti, dilaksana dan dikaji secara berkala; e) jalinan perhubungan/komunikasi dengan pihak yang relevan hendaklah dipelihara; dan f) kajian semula ke atas keselamatan siber hendaklah dijalankan mengikut peraturan yang ditetapkan.	JPICT JPPM, JPPM CSIRT dan Jawatankuasa Kajian Semula Pengurusan ISMS JPPM

020102 Ketua Pengarah JPPM

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

a) menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber JPPM;
b) melantik CDO dan ICTSO;
c) memantau pelaksanaan dan pematuhan PKS JPPM melalui CDO;
d) memperuntukkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi memastikan arah tuju dan strategi keselamatan siber JPPM dapat dilaksanakan; dan
e) mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT JPPM.

020103 Ketua Pegawai Digital (CDO)

Ketua Pegawai Digital (CDO) berperanan dan bertanggungjawab seperti berikut: — CDO

a) membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber sebagaimana yang ditetapkan di dalam PKS JPPM;
b) kawalan keselamatan maklumat di JPPM hendaklah diseragamkan dan diselaraskan dengan sebaiknya;
c) Pelan Strategik ICT JPPM hendaklah mengandungi aspek keselamatan siber;
d) melantik ahli pasukan JPPM CSIRT;
e) meneraju inisiatif pendigitalan di JPPM melalui penggunaan data, analitis dan teknologi digital;
f) mewujudkan budaya berpacukan data dalam Sektor Awam yang mengamalkan pendekatan *principle-based* melalui

penggunaan data dan teknologi digital;

g) mentransformasi penyampaian perkhidmatan digital di JPPM berfokuskan pengalaman pelanggan (*customer experience*) yang berteraskan konsep *Whole-of-Government* melalui inovasi melibatkan perkongsian data, data terbuka dan teknologi baharu;

h) menilai, menyelaras dan memperaku keperluan perkhidmatan digital, *Technical Service Design,* bajet pembangunan serta mengurus JPPM sebagai pelaksana inisiatif dan projek pendigitalan;

i) meneraju perubahan melalui Penjajaran Pelan Strategik ICT (PSICT)/Pelan Strategik Pendigitalan (PSP) JPPM dengan memastikan perkara-perkara berikut:

- PSICT/PSP JPPM hendaklah selari dengan PSICT/PSP Sektor Awam dan Pengurusan Risiko serta Pelan Pengurusan Perubahan;
- *Blueprint Enterprise Architecture* (EA) JPPM hendaklah tersedia; dan
- memantapkan struktur tadbir urus pendigitalan JPPM serta menyelaras penggunaan dasar, standard dan amalan terbaik global.

j) melaporkan pelaksanaan dan kemajuan transformasi pendigitalan kepada Ketua Pengarah.

020104 Pegawai Keselamatan ICT (ICTSO)

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: ICTSO

a) menguatkuasakan dan memantau pelaksanaan PKS JPPM;

b) memastikan semua infrastruktur keselamatan siber JPPM hendaklah menepati prinsip-prinsip keselamatan berpandukan PKS JPPM dan Arahan Keselamatan;

c) menyediakan dan mengkaji semula dokumen infrastruktur keselamatan siber JPPM bagi tujuan audit keselamatan siber;
d) mengenal pasti bidang-bidang keselamatan siber JPPM yang perlu diberikan perhatian;
e) memastikan tahap keselamatan siber JPPM adalah terjamin setiap masa;
f) memastikan semua warga JPPM memahami keperluan standard, garis panduan dan prosedur keselamatan di bawah PKS JPPM;
g) menjalankan penilaian risiko dan program-program keselamatan siber di JPPM;
h) mewujudkan pelan tindakan bagi mengurus risiko akibat daripada ketidakpatuhan kepada standard, garis panduan dan polisi keselamatan siber di JPPM;
i) melaporkan kepada JPPM CSIRT, KDN CSIRT seterusnya NACSA mengenai sebarang insiden keselamatan siber yang berlaku di JPPM;
j) bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera;
k) membantu dalam membangunkan standard, garis panduan dan prosedur untuk aplikasi, sistem dan infrastruktur ICT di JPPM bagi mematuhi keperluan PKS JPPM;
l) mewujudkan program-program bagi meningkatkan pengetahuan, kesedaran dan pembudayaan mengenai peranan dan tanggungjawab warga JPPM dalam mengendalikan kemudahan ICT di JPPM teknologi termasuklah mekanisme kawalan terhadap maklumat, aset ICT dan ancaman siber;
m) menyebarkan dan menyalurkan amaran awal terhadap ancaman-ancaman yang berpotensi menyebabkan kerosakan besar kepada aset ICT JPPM; dan

n) menyelaras serta mengurus pelan latihan/program kesedaran keselamatan siber di JPPM.

020105 Jawatankuasa Pemandu ICT JPPM

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

Jawatankuasa Keselamatan ICT JPPM

Keanggotaan Jawatankuasa Pemandu ICT JPPM adalah seperti berikut:

Pengerusi: Ketua Pengarah

Ahli:

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

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

Bidang Kuasa:

a) menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT JPPM;
b) merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT JPPM;
c) merancang dan menyelaras pembangunan dan pelaksanaan program/projek ICT JPPM supaya selaras dengan Pelan Strategik ICT JPPM;
d) menyelaras dan menyeragamkan pembangunan ICT JPPM agar selari dengan Pelan Strategik JPPM dan Pelan

Strategik ICT JPPM;

e) menilai dan meluluskan projek ICT JPPM berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan;
f) mengikuti dan memantau perkembangan program ICT JPPM serta memahami keperluan, masalah dan isu yang dihadapi dalam pembangunan dan pelaksanaan ICT;
g) merancang dan menentukan langkah-langkah keselamatan ICT;
h) menyelaras dan mengemukakan perolehan ICT yang telah diluluskan di peringkat JPICT JPPM kepada JPICT KDN untuk kelulusan; dan
i) mengemukakan laporan kemajuan projek ICT yang telah diluluskan oleh JTISA (sekiranya berkaitan) kepada JPICT KDN mengikut tempoh yang telah ditetapkan.
j) memperakui pelaksanaan pensijilan ISO/IEC 27001:2013 *Information Security Management System* (ISMS) dan makluman status kemajuan ISMS.

020106 Jawatankuasa Kajian Semula Pengurusan ISMS JPPM

Jawatankuasa Kajian Semula Pengurusan ISMS JPPM dipengerusikan oleh Timbalan Ketua Pengarah JPPM yang bertanggungjawab terhadap hal ehwal pengurusan ISMS JPPM.

Jawatankuasa Kajian Semula Pengurusan ISMS JPPM

Keanggotaan Jawatankuasa Kajian Semula Pengurusan ISMS JPPM adalah seperti yang berikut:

Pengerusi: Timbalan Ketua Pengarah (CDO JPPM)

Ahli:

1. Pengarah BPTM (ICTSO)
2. Pengarah Bahagian Sumber Manusia dan Khidmat

Pengurusan

3. Pengarah Bahagian Pengurusan Pertubuhan
4. Pengarah-Pengarah JPPM Negeri yang dilantik
5. Penolong Pengarah BPTM

Urus setia bagi Jawatankuasa Kajian Semula Pengurusan ISMS JPPM adalah Pasukan Penyelaras ISMS JPPM.

Bidang Kuasa:

a) memantau dan menyemak pelaksanaan pensijilan ISMS;
b) menetapkan struktur organisasi ISMS;
c) menetap kriteria penerimaan risiko, tahap risiko dan risk treatment plan;
d) melaksana Mesyuarat Kajian Semula Pengurusan (MKSP) ISMS JPPM sekurang-kurangnya dua (2) kali setahun (sekali dalam masa enam (6) bulan pertama dan sekali dalam masa enam (6) bulan kedua); dan
e) mengemukakan cadangan perolehan ICT berkaitan keselamatan maklumat JPPM kepada JPICT JPPM untuk kelulusan.

020107 Bahagian Pengurusan Teknologi Maklumat (BPTM)

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

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

Bidang Kuasa:

a) memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam JPPM yang mematuhi

keperluan PKS JPPM;

b) menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan siber;
c) memastikan PKS JPPM selaras dengan dasar-dasar ICT kerajaan semasa;
d) menerima laporan dan membincangkan hal-hal keselamatan siber semasa; dan
e) membuat keputusan mengenai tindakan yang perlu diambil mengenai sebaran insiden.

020108 Pentadbir ICT

Peranan dan tanggungjawab Pentadbir ICT adalah seperti berikut: Pentadbir ICT

a) memastikan kerahsiaan akaun pentadbir;
b) menjaga kerahsiaan konfigurasi aset ICT;
c) mengambil tindakan dengan segera apabila dimaklumkan mengenai warga JPPM yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
d) mengambil tindakan dengan segera apabila dimaklumkan mengenai pihak ketiga yang berhenti atau tamat projek;
e) menentukan ketepatan dan kesempurnaan sesuatu tahap akses sebagaimana yang telah ditetapkan di dalam PKS JPPM;
f) memantau aktiviti akses sistem aplikasi warga JPPM;
g) mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran serta membatalkan atau memberhentikannya dengan serta merta dan memaklumkan kepada ICTSO untuk tindakan selanjutnya;
h) menganalisis dan menyimpan rekod jejak audit; dan
i) memastikan pembangunan sistem aplikasi mengambil kira

dan mematuhi ciri-ciri keselamatan yang dinyatakan di dalam PKS JPPM.

020109 Warga JPPM

Warga JPPM mempunyai peranan dan tanggungjawab seperti berikut: Warga JPPM

a) menjaga kerahsiaan maklumat JPPM yang meliputi maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;
b) melaksanakan dan mematuhi prinsip-prinsip PKS JPPM serta menjaga kerahsiaan maklumat JPPM;
c) mengetahui dan memahami implikasi keselamatan siber daripada tindakannya;
d) menjaga kerahsiaan kata laluan (*password*);
e) menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rahsia rasmi;
f) melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ahli pasukan JPPM CSIRT dengan segera;
g) menghadiri program-program kesedaran mengenai keselamatan siber; dan
h) membaca, memahami dan membuat perakuan melalui Portal Intranet JPPM.

0202 Pihak Ketiga

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (pembekal, pakar runding dan lain-lain).

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal.	CDO, ICTSO, Pentadbir ICT dan Pihak Ketiga
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	

a) melaksanakan dan mematuhi prinsip-prinsip PKS JPPM serta menjaga kerahsiaan maklumat JPPM;
b) mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran akses;
c) mengenal pasti keperluan keselamatan sebelum memberi kebenaran akses atau penggunaan kepada pihak ketiga;
d) akses kepada aset ICT JPPM perlu berlandaskan kepada perjanjian kontrak;
e) semua syarat keselamatan berikut hendaklah dilengkapkan oleh pihak ketiga:
    a. Perakuan Akta Rahsia Rasmi 1972;
    b. Akuan Pematuhan PKS JPPM;
    c. Tapisan Keselamatan *(e-Vetting);* dan
    d. Hak Harta Intelek (dinyatakan di dalam perjanjian).
f) membaca, memahami dan membuat perakuan melalui Portal Intranet JPPM.

020202 Keselamatan Maklumat dalam Pengurusan Projek

Memastikan setiap pengurusan projek (tanpa mengira jenis projek) yang dilaksanakan oleh JPPM mengambil kira aspek keselamatan maklumat secara holistik.	Warga JPPM (Pasukan Projek)

Warga JPPM (Pasukan Projek) adalah bertanggungjawab untuk:

a) menjadikan objektif keselamatan maklumat sebahagian daripada objektif projek;
b) pengurusan projek hendaklah mematuhi manual keselamatan dan PKS JPPM dalam setiap aktiviti pengurusan projek; dan
c) semua pihak yang terlibat dalam sesuatu projek perlu maklum tentang arahan berkaitan keselamatan maklumat dan mereka terikat dengan perjanjian (seperti Akta Rahsia Rasmi 1972).

0203 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif:

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

020301 Pengguna Peralatan Mudah Alih

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Warga JPPM

a) tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;
b) peralatan mudah alih hendaklah sentiasa dikunci dengan

menggunakan *cable lock;*

c) peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan
d) tindakan perlindungan diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan akses tidak sah serta salah guna kemudahan.

020302 Kerja Jarak Jauh

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Warga JPPM

a) tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan akses tidak sah serta salah guna kemudahan;
b) akses rangkaian kerja jarak jauh untuk tujuan rasmi perlu didaftarkan dan perlu mematuhi peraturan semasa; dan
c) warga JPPM tertakluk kepada prinsip-prinsip yang menjadi asas kepada PKS JPPM dan perlu dipatuhi.

020303 Bawa Peranti Sendiri (BYOD)

Pengguna BYOD perlu mematuhi perkara-perkara seperti berikut: Warga JPPM dan Pihak Ketiga

a) peranti peribadi yang dibenarkan oleh ICTSO untuk digunakan seperti komputer riba, telefon pintar dan tablet untuk tujuan rasmi perlu mematuhi peraturan semasa; dan
b) semua peringkat maklumat rasmi Kerajaan adalah hak milik Kerajaan.

Pengguna BYOD tertakluk kepada tatacara penggunaan peranti peribadi seperti berikut:

a) warga JPPM dan pihak ketiga adalah bertanggungjawab menggunakan peranti milik sendiri secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/dasar yang berkuat kuasa;
b) warga JPPM dan pihak ketiga bertanggungjawab untuk memadamkan segala maklumat yang berkaitan dengan urusan rasmi JPPM di dalam peranti peribadi sekiranya bertukar/ditamatkan perkhidmatan/bersara atau sewaktu dihantar ke pusat servis untuk penyelenggaraan;
c) warga JPPM adalah bertanggungjawab dan boleh dikenakan tindakan tatatertib sekiranya didapati menyalahgunakan peranti peribadi yang menyebabkan kehilangan/kerosakan/pendedahan maklumat rasmi Kerajaan;
d) JPPM tidak bertanggungjawab atas kehilangan atau kerosakan peranti peribadi yang digunakan untuk tujuan urusan rasmi JPPM; dan
e) peranti mudah alih yang merupakan aset JPPM tidak tertakluk kepada dasar ini. Warga JPPM tersebut masih tertakluk kepada langkah-langkah perlindungan keselamatan yang berkuatkuasa.
f) pengguna BYOD adalah dilarang daripada melakukan perkara-perkara berikut:
    - menggunakan peranti peribadi untuk mengakses, menyimpan dan menyebarkan maklumat rasmi Kerajaan kepada pihak yang tidak dibenarkan;
    - penggunaan peranti peribadi untuk tujuan peribadi yang boleh menggangu produktiviti kerja;

- menjadikan peranti peribadi sebagai medium sandaran (*backup*) bagi maklumat rasmi Kerajaan;
- merakam komunikasi dan maklumat rasmi Kerajaan untuk tujuan peribadi; dan
- menjadikan peranti peribadi sebagai *access point* kepada aset ICT JPPM untuk akses ke Internet.

g) pengguna BYOD perlu memastikan peranti peribadi yang digunakan mempunyai kawalan keselamatan seperti berikut:

- menetapkan mekanisme kawalan akses bagi peranti peribadi dan akan mengunci secara automatik apabila tidak digunakan;
- melaksanakan enkripsi dan/atau perlindungan ke atas *folder* yang mempunyai maklumat rasmi Kerajaan yang disimpan di dalam peranti milik sendiri; dan
- memuat turun aplikasi daripada sumber yang sah.

BIDANG 03 KESELAMATAN SUMBER MANUSIA

0301 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

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

030101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi adalah seperti berikut: — ICTSO, BSMKP, Warga JPPM, dan Pihak Ketiga

a) menyatakan dengan jelas peranan dan tanggungjawab warga JPPM serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
b) menjalankan tapisan keselamatan untuk warga JPPM serta pihak ketiga yang terlibat berdasarkan keperluan perundangan, peraturan dan etika yang terpakai selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan diakses serta risiko yang dijangkakan; dan
c) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan serta peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

030102 Dalam Perkhidmatan

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:	ICTSO, BSMKP, Warga JPPM dan Pihak Ketiga
a) warga JPPM serta pihak ketiga yang berkepentingan hendaklah mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh JPPM;	
b) kesedaran mengenai pengurusan keselamatan aset ICT hendaklah diberikan kepada warga JPPM secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;	
c) proses tindakan disiplin dan/atau undang-undang ke atas warga JPPM serta pihak ketiga yang berkepentingan hendaklah diwujudkan sekiranya berlaku pelanggaran dengan perundangan dan peraturan berkuat kuasa; 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 siber. Sebarang kursus dan latihan teknikal yang diperlukan, warga JPPM boleh merujuk kepada Bahagian Sumber Manusia dan Khidmat Pengurusan (BSMKP), JPPM.	

030103 Bertukar atau Tamat Perkhidmatan

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:	ICTSO, BSMKP, Pentadbir ICT dan Warga JPPM
a) semua aset ICT hendaklah dikembalikan kepada JPPM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan	
b) membatalkan atau menarik balik semua kebenaran akses ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan.	

BIDANG 04 PENGURUSAN ASET

0401 Akauntabiliti Aset

Objektif:

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

040101 Inventori Aset ICT

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

BPTM dan Warga JPPM

Perkara yang perlu dipatuhi adalah seperti berikut:

a) maklumat semua aset ICT dikenal pasti, direkodkan dan sentiasa dikemas kini;
b) semua aset ICT mempunyai pemilik dan dikendalikan oleh warga JPPM yang dibenarkan sahaja;
c) lokasi semua aset ICT dikenal pasti dan direkodkan;
d) peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan
e) setiap warga JPPM adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

0402 Pengelasan dan Pengendalian Maklumat

Objektif:

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

040201 Pengelasan dan Pelabelan Maklumat

Maklumat rahsia rasmi hendaklah dikelaskan oleh Pegawai Pengelas dan ditandakan sebagaimana yang ditetapkan di dalam Arahan Keselamatan seperti berikut: — Warga JPPM

a) Rahsia Besar;
b) Rahsia;
c) Sulit; atau
d) Terhad.

040202 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: — Warga JPPM

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 yang sedia untuk digunakan;
d) menjaga kerahsiaan kata laluan;
e) mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
f) memberi perhatian kepada maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, membuat salinan, pertukaran dan pemusnahan; dan
g) menjaga kerahsiaan langkah-langkah keselamatan siber dari diketahui umum.

0403 Pengendalian Media

Objektif:

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

040301 Pengurusan Media Boleh Alih

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — Warga JPPM dan Pihak Ketiga

a) mengehadkan dan menentukan akses media storan kepada warga JPPM dan pihak ketiga yang dibenarkan sahaja;
b) mengehadkan pengedaran data atau media storan untuk tujuan yang dibenarkan sahaja;
c) mengawal media storan daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan;
d) menyimpan semua media storan di tempat yang selamat serta bersesuaian dengan kandungan maklumat;
e) akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada warga JPPM dan pihak ketiga yang dibenarkan sahaja; dan
f) media storan yang mengandungi maklumat rahsia rasmi hendaklah disanitasi sebelum dihapuskan atau dimusnahkan mengikut prosedur yang ditetapkan.

040302 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media storan yang mengandungi maklumat rahsia rasmi ke luar pejabat hendaklah dikawal. — Warga JPPM

BIDANG 05 KAWALAN AKSES

0501 Dasar Kawalan Akses

Objektif:

Mengawal akses ke atas maklumat.

050101 Keperluan Kawalan Akses

Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan akses pengguna sedia ada. Peraturan kawalan akses hendaklah diwujudkan, didokumenkan dan dikaji semula berdasarkan keperluan perkhidmatan dan keselamatan.	CDO, ICTSO, BPTM, dan Pentadbir ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

0502 Pengurusan Akses Pengguna

Objektif:

Mengawal akses pengguna ke atas aset ICT JPPM.

050201 Akaun Pengguna

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. 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 ICT boleh membeku, mengehadkan atau menamatkan akaun pengguna atas sebab-sebab berikut: i. pengguna bertukar jawatan, tanggungjawab dan/atau dikenakan tindakan tatatertib; dan ii. pengguna bertukar agensi, bersara dan/atau tamat perkhidmatan.	ICTSO, Pentadbir ICT dan Warga JPPM

050202 Hak Akses

Penetapan dan penggunaan ke atas hak akses perlu diberi kawalan dan penyeliaan yang sewajarnya berdasarkan keperluan skop tugas.	ICTSO dan Pentadbir ICT

050203 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mengakses maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JPPM seperti berikut:	ICTSO, Pentadbir ICT dan Warga JPPM

a) dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;
b) warga JPPM 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 sistem pengoperasian dan *screen saver* hendaklah diaktifkan terutamanya pada komputer dan komputer riba yang terletak di ruang kerja warga JPPM serta server di pusat data yang menempatkan sistem aplikasi JPPM;
f) kata laluan hendaklah dimasukkan dalam bentuk yang tidak boleh dilihat, tidak dipaparkan dalam laporan atau media lain serta 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) sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.

0503 Kawalan Akses Rangkaian

Objektif:

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

050301 Keperluan Kawalan Akses

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

a) menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian JPPM, rangkaian agensi lain dan rangkaian awam;
b) mewujudkan serta menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan
c) memantau dan menguatkuasakan kawalan akses pengguna terhadap perkhidmatan rangkaian ICT.

050302 Akses Internet

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — ICTSO, Pentadbir ICT, dan warga JPPM

a) penggunaan Internet di JPPM hendaklah dipantau secara berterusan oleh Pentadbir ICT bagi memastikan penggunaannya untuk tujuan akses yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan kod/perisian hasad, 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 untuk mengawal aktiviti (*video conferencing, video streaming, chat,* muat turun) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang optimum 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;

e) bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan/pegawai yang diberi kuasa sebelum dimuat naik ke Internet;

f) warga JPPM hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

g) sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh JPPM;

h) penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

i) warga JPPM adalah dilarang melakukan aktiviti-aktiviti seperti berikut:

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

   ii. menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur pornografi, perjudian atau keganasan.

0504 Kawalan Akses Sistem Pengoperasian

Objektif:

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

050401 Akses Sistem Pengoperasian

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

ICTSO dan Pentadbir ICT

a) mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan
b) merekodkan akses yang berjaya dan gagal.

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

a) mengesahkan pengguna yang dibenarkan;
b) mewujudkan jejak audit ke atas semua akses sistem pengoperasian terutama pengguna bertaraf *super user;* dan
c) menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) mengawal akses 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) mengehadkan dan mengawal penggunaan program; dan
d) mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

0505 Kawalan Akses Aplikasi dan Maklumat

Objektif:

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

050501 Akses Aplikasi dan Maklumat

Memastikan sistem aplikasi dan maklumat sedia ada dilindungi dari sebarang bentuk akses yang tidak dibenarkan yang boleh menyebabkan kerosakan. — ICTSO dan Pentadbir ICT

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

a) warga JPPM hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap akses serta keselamatan maklumat yang telah ditentukan;
b) setiap aktiviti akses sistem maklumat dan aplikasi warga JPPM hendaklah direkodkan (sistem log);
c) mengehadkan akses sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau akses pengguna akan disekat; dan
d) kawalan akses sistem dan aplikasi hendaklah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau akses yang tidak sah.

0506 Kawalan Akses Pangkalan Data

Objektif:

Menghalang akses tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam pangkalan data.

050601 Akses Pangkalan Data

Akses ke atas pangkalan data hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong pengesahan pengguna, mewujudkan jejak audit ke atas semua akses, pengesahan akses dan penyimpanan data. ICTSO dan Pentadbir ICT

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

a) akses ke atas pangkalan data hendaklah dikawal;
b) penggunaan perisian yang membolehkan akses terus ke pangkalan data oleh pihak ketiga sama ada melalui perisian web (contoh: *phpmyadmin*) atau sebagainya hendaklah dikawal;
c) mewujudkan pengenalan diri (ID) yang unik bagi setiap pengguna dan hanya digunakan untuk pengguna berkenaan sahaja; dan
d) aplikasi yang perlu mengakses ke pangkalan data perlu menggunakan pengenalan diri yang berbeza daripada pengenalan diri pembangun aplikasi dan pentadbir pangkalan data.

BIDANG 06 KAWALAN KRIPTOGRAFI

0601 Kawalan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

060101 Enkripsi (*Encryption)*

Penghantaran maklumat rahsia rasmi secara elektronik hendaklah dilaksanakan menggunakan kaedah enkripsi (*encryption*) mengikut kesesuaian.

ICTSO dan Warga JPPM

060102 Pengurusan Infrastruktur Kunci Awam (PKI)

Pengurusan ke atas Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

Pentadbir ICT, Warga JPPM dan Pihak Ketiga

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) penggunaan sijil digital bagi akses sistem hendaklah mengikut kesesuaian dan keperluan keselamatan siber;
b) sijil digital hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;
c) perkongsian sijil digital untuk sebarang akses sistem adalah tidak dibenarkan sama sekali; dan
d) sebarang perubahan kepada pemilik atau kehilangan/ kerosakan hendaklah dilaporkan kepada pemilik Infrastruktur Kunci Awam (PKI) berkenaan.

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Kawasan Selamat (*Secure Area*)

Objektif:

Menghalang akses fizikal yang tidak dibenarkan yang mana boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat JPPM.

070101 Perimeter Keselamatan Fizikal

Perimeter keselamatan fizikal diperlukan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat JPPM. — CDO, ICTSO, BPTM dan BSMKP

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) kawalan keselamatan fizikal hendaklah dikenal pasti dengan jelas;
b) lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
c) menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
d) memasang alat penggera atau kamera keselamatan;
e) mengehadkan jalan keluar masuk;
f) mengadakan kaunter kawalan;
g) menyediakan ruangan atau bilik khas untuk pelawat;
h) mewujudkan kawalan keselamatan fizikal;
i) melindungi kawasan selamat melalui kawalan pintu masuk yang bersesuaian bagi memastikan warga JPPM yang

diberi kebenaran sahaja boleh melalui pintu masuk ini;

j) mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan yang disediakan;

k) mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan sebarang bencana alam atau perbuatan manusia; dan

l) kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain hendaklah dikawal daripada pihak yang tidak diberikan kebenaran memasukinya.

070102 Kawalan Kemasukan Fizikal

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: CDO, ICTSO, Warga JPPM, Pihak Ketiga dan Pelawat

a) setiap warga JPPM hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas di premis JPPM;

b) semua pas keselamatan hendaklah diserahkan balik kepada BSMKP, JPPM apabila warga JPPM bertukar keluar, berhenti atau bersara;

c) setiap pihak ketiga dan pelawat perlu mendaftar serta mendapatkan pas pelawat di pintu masuk ke kawasan atau tempat berurusan. Pas tersebut perlu dikembalikan semula selepas tamat urusan di premis JPPM;

d) kehilangan pas mestilah dilaporkan dengan segera; dan

e) hanya warga JPPM, pihak ketiga dan pelawat yang diberi kebenaran sahaja boleh mengakses atau menggunakan aset ICT JPPM.

070103 Bekerja di Kawasan Selamat

Kawasan selamat dikenal pasti sebagai kawasan yang dihadkan kemasukan bagi warga JPPM yang tertentu sahaja. ICTSO, BSMKP, Pentadbir ICT

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam.

Kawalan-kawalan keselamatan ke atas kawasan tersebut adalah seperti berikut:

a) sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuklah sistem pencegahan kebakaran;
b) akses adalah terhad kepada warga JPPM yang telah diberi kuasa sahaja dan dipantau pada setiap masa;
c) pemantauan dibuat menggunakan kamera *Closed-Circuit Television* (CCTV) atau lain-lain peralatan yang sesuai;
d) peralatan keselamatan termasuklah CCTV dan log akses perlu diperiksa secara berjadual;
e) butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;
f) pelawat yang dibawa masuk mesti diawasi oleh pengawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;
g) lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam;
h) memperkukuh dinding dan siling; dan
i) mengehadkan jalan keluar masuk.

0702 Keselamatan Peralatan ICT

Objektif:

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

070201 Penempatan dan Perlindungan Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: ICTSO, Pentadbir ICT dan Warga JPPM

a) warga JPPM hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;
b) warga JPPM bertanggungjawab sepenuhnya ke atas peralatan ICT di bawah jagaannya dan tidak dibenarkan membuat sebarang pengubahsuaian komponen, konfigurasi dan lokasi yang telah ditetapkan serta menggunakan sepenuhnya bagi urusan rasmi sahaja;
c) warga JPPM dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan ICT yang telah ditetapkan;
d) warga JPPM dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir ICT;
e) warga JPPM adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;
f) warga JPPM mesti memastikan perisian antivirus di komputer di bawah kawalannya sentiasa aktif dan dikemas kini serta imbasan dilaksanakan secara berkala;
g) penggunaan kata laluan untuk akses ke komputer, komputer riba, server dan media mudah alih yang mengandungi maklumat rahsia rasmi adalah diwajibkan;
h) peralatan-peralatan ICT yang kritikal seperti server perlu disokong oleh *Uninterruptable Power Supply* (UPS);
i) 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;
j) semua peralatan ICT yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin atau

mempunyai pengudaraan (*air ventilation*) yang sesuai;

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

l) pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

m) laporkan kehilangan peralatan ICT kepada ICTSO dengan segera;

n) sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada pegawai yang bertanggungjawab untuk dibaik pulih;

o) sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

p) warga JPPM dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan;

q) konfigurasi alamat IP dilarang diubah daripada alamat IP yang telah ditetapkan;

r) warga JPPM hendaklah memastikan semua perkakasan komputer, komputer riba, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan premis JPPM;

s) sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan

t) semua pergerakan peralatan ICT JPPM hendaklah direkodkan.

070202 Penyelenggaraan Peralatan ICT

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) semua peralatan ICT yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan;
b) peralatan ICT diselenggara oleh Pentadbir ICT atau pihak yang dibenarkan sahaja;
c) semua peralatan ICT hendaklah diselenggara sama ada dalam tempoh jaminan atau setelah habis tempoh jaminan;
d) semua peralatan ICT hendaklah disemak/diuji sebelum dan selepas proses penyelenggaraan;
e) penyelenggaraan peralatan ICT hendaklah mendapat kebenaran daripada Pentadbir ICT berkenaan;
f) aktiviti penyelenggaraan peralatan ICT hendaklah direkodkan; dan
g) memaklumkan warga JPPM sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

070203 Peminjaman Peralatan ICT Untuk Kegunaan Di Luar Pejabat

Peralatan ICT yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan peralatan ICT:

Pentadbir ICT dan Warga JPPM

a) peralatan ICT yang dibawa keluar premis JPPM hendaklah mendapat kelulusan Pentadbir ICT dan tertakluk kepada tujuan yang dibenarkan; dan
b) aktiviti peminjaman dan pemulangan peralatan ICT hendaklah direkodkan.

070204 Peralatan ICT di Luar Premis

Peralatan ICT yang terletak di luar premis JPPM adalah terdedah kepada pelbagai risiko. — Warga JPPM

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) peralatan ICT perlu dilindungi dan dikawal sepanjang masa;
b) penyimpanan atau penempatan peralatan ICT hendaklah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan
c) kehilangan peralatan ICT hendaklah dilaporkan mengikut peraturan semasa yang ditetapkan.

070205 Pelupusan Peralatan ICT

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya keselamatan maklumat terjamin. — Pegawai Aset, BPTM dan Warga JPPM

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) semua kandungan peralatan ICT khususnya yang mengandungi maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum dilupuskan sama ada melalui kaedah:
    i. penyingkiran (*purging*) seperti *secure erase* atau *degaussing*;
    ii. pemusnahan media secara fizikal (*destroying*) seperti penghancuran (*disintegration*), kisaran halus (*pulverization)*, peleburan atau pembakaran; dan
    iii. merujuk kepada Portal Pekeliling Perbendaharaan.

b) sekiranya maklumat perlu disimpan, warga JPPM boleh membuat penduaan;
c) data-data dalam storan peralatan ICT hendaklah dihapuskan dengan cara yang selamat;
d) Pengawai Pengeluar (PEP) mengenal pasti sama ada peralatan ICT tertentu boleh dilupuskan atau sebaliknya;
e) Pegawai Aset bertanggungjawab merekodkan butiran pelupusan dan mengemas kini rekod pelupusan peralatan ICT;
f) peralatan ICT yang hendak dilupuskan disimpan di tempat yang telah dikhaskan dan mempunyai ciri-ciri keselamatan; dan
g) warga JPPM adalah dilarang sama sekali daripada melakukan perkara-perkara seperti berikut:
    i. menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;
    ii. mencabut, menanggal dan menyimpan komponen peralatan ICT seperti RAM, *hard disk*, *motherboard* dan sebagainya;
    iii. memindah keluar peralatan ICT yang hendak dilupuskan dari JPPM; dan
    iv. melupuskan sendiri peralatan ICT.

0703 Keselamatan Persekitaran

Objektif:

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

070301 Kawalan Persekitaran

Bagi menghindari kerosakan dan gangguan terhadap premis serta peralatan ICT, semua cadangan berkaitan premis sama

Unit Khidmat Pengurusan,

	ada untuk memperoleh, menyewa, ubah suai atau pembelian hendaklah mematuhi garis panduan, tatacara dan prosedur yang sedang berkuat kuasa.	Pentadbir ICT dan Warga JPPM
	Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: a) merancang dan menyediakan pelan keseluruhan susun atur pusat data dengan teliti; b) semua ruang pejabat khususnya kawasan yang mempunyai peralatan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pengesan kebakaran, alat pemadam kebakaran dan pintu kecemasan; c) peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dikenal pasti dan dikendalikan; d) bahan mudah terbakar hendaklah disimpan di luar kawasan penyimpanan peralatan ICT; e) semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari peralatan ICT; f) warga JPPM adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT; 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.	
070302	**Bekalan Kuasa**	
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.	Pentadbir ICT dan Unit

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Khidmat Pengurusan

a) semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik;
b) peralatan sokongan seperti 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.

070303 Keselamatan Kabel

Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi bagi mengelakkan maklumat terdedah kepada ancaman. Pentadbir ICT

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.

070304 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Unit Khidmat Pengurusan

a) warga JPPM hendaklah memahami dan mematuhi

	prosedur kecemasan JPPM yang berkuat kuasa; dan b) kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan yang dilantik.	dan Warga JPPM
070305	***Clear Desk* dan *Clear Screen***	
	Semua maklumat dalam apa jua bentuk 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 di atas meja warga JPPM atau di paparan skrin apabila warga JPPM tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) menggunakan kemudahan *password screen lock*/*screen saver* sekurang-kurangnya 10 minit atau *logout* apabila meninggalkan komputer; b) menyimpan bahan dan maklumat rahsia rasmi di dalam laci atau kabinet fail yang berkunci; dan c) semua dokumen hendaklah diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Warga JPPM
0704	**Keselamatan Dokumen**	
	Objektif: Melindungi maklumat JPPM daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, pencerobohan, kemalangan atau kecurian.	

070401 Kawalan Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Warga JPPM

a) setiap dokumen rahsia rasmi hendaklah difailkan dan dilabelkan mengikut klasifikasi dokumen seperti Rahsia Besar, Rahsia, Sulit, atau Terhad;
b) pergerakan fail dan dokumen hendaklah direkodkan serta perlulah mengikut prosedur yang ditetapkan;
c) kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut Arahan Keselamatan;
d) pelupusan dokumen hendaklah mengikut prosedur yang berkuat kuasa seperti Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan
e) menggunakan kata laluan atau enkripsi (*encryption*) ke atas dokumen/rekod elektronik rahsia rasmi.

070402 Keselamatan Sistem Dokumentasi

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

a) sistem penyimpanan dokumentasi hendaklah mempunyai ciri-ciri keselamatan;
b) menyedia dan memantapkan keselamatan sistem dokumentasi; dan
c) mengawal serta merekodkan semua aktiviti akses dokumentasi sedia ada.

BIDANG 08 KESELAMATAN OPERASI

0801 Pengurusan Prosedur Operasi

Objektif:

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

080101 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

ICTSO, Pentadbir ICT dan Warga JPPM

a) semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan serta 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 serta pemulihan sekiranya pemprosesan tergendala atau terhenti;
c) semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan; dan
d) warga JPPM hendaklah mematuhi prosedur yang telah ditetapkan.

080102 Kawalan Perubahan

Perubahan dalam organisasi, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal.

ICTSO, Pentadbir ICT dan Warga JPPM

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) pengubahsuaian yang melibatkan peralatan ICT, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau Pentadbir ICT terlebih dahulu;
b) aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT (perkakasan, perisian, sistem aplikasi, pangkalan data dan maklumat) hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa serta mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
c) semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
d) semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.

080103 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: ICTSO dan Pentadbir ICT

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 dan mengesahkan maklumat hendaklah diasingkan bagi mengelakkan daripada akses yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat rahsia rasmi atau dimanipulasi; dan
c) pembangunan, pengujian dan operasi (penggunaan) mesti diasingkan bagi mengurangkan risiko akses atau

pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

080104 Pengurusan Kapasiti

Bagi meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem, perkara-perkara berikut perlu dipatuhi: — ICTSO dan Pentadbir ICT

a) kapasiti sesuatu aset ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang bertanggungjawab bagi memastikan keperluannya adalah mencukupi serta bersesuaian untuk pembangunan dan kegunaan pada masa akan datang; dan
b) keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

0802 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

080201 Penerimaan Sistem

Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. — ICTSO, Pentadbir ICT dan Pemilik Projek

0803 Perisian Hasad (*Malware*)

Objektif:

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

080301 Perlindungan dari Perisian Hasad

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: ICTSO, Pentadbir ICT, Pihak Ketiga dan Warga JPPM

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 antivirus sebelum menggunakannya;
d) mengemas kini *signature* dan versi perisian keselamatan 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 dan jaminan kualiti di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

h) memaklumkan kepada warga JPPM mengenai ancaman keselamatan ICT seperti serangan virus; dan
i) penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

0804 Sandaran (*Backup*)

Objektif:

Melindungi ketersediaan maklumat dan perkhidmatan agar boleh diakses pada bila-bila masa dan memastikan segala maklumat diselenggara agar penyimpanan maklumat diuruskan dengan sempurna.

080401 Sandaran Maklumat (*Backup*)

Perkara-perkara berikut perlu dipatuhi bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana: — ICTSO dan Pentadbir ICT

a) melaksanakan *backup* dan menguji secara berkala mengikut prosedur yang telah ditetapkan;
b) melaksanakan *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung kepada tahap kritikal maklumat;
c) menguji *backup* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana;
d) menyimpan sekurang-kurangnya tiga (3) generasi *backup* kecuali bagi sistem yang tidak mempunyai penambahan data; dan
e) merekod serta menyimpan salinan *backup* di lokasi yang berlainan dan selamat.

0805 Pengelogan dan Pemantauan

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan serta merekodkan peristiwa dan menghasilkan bukti.

080501 Pengelogan Kejadian

Pentadbir ICT

Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT adalah bukti yang direkodkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap akses yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.

Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut:

a) fail log sistem pengoperasian;
b) fail log servis (contoh: web, e-mel);
c) fail log aplikasi (audit trail); dan
d) fail log rangkaian (contoh: *switch, firecall, IPS*).

Pentadbir ICT hendaklah melaksanakan perkara-perkara berikut:

a) mewujudkan sistem log bagi merekodkan semua aktiviti

harian pengguna;

b) menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan

c) sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan kepada ICTSO dan CDO.

080502 Perlindungan Maklumat Log

Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan akses tanpa izin. — ICTSO dan Pentadbir ICT

080503 Log Pentadbir dan Pengendali

Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan serta log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap. Aktiviti-aktiviti yang perlu dilaksanakan adalah seperti berikut: — ICTSO dan Pentadbir ICT

a) memantau penggunaan kemudahan memproses maklumat secara berkala;

b) aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa serta menyediakan laporan jika perlu;

c) kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;

d) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan serta memantau kawalan akses; dan

e) sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan kepada pasukan MAMPU CSIRT.

080504 Penyeragaman Jam

Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.	ICTSO dan Pentadbir ICT
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JPPM atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh National Metrology Institute of Malaysia (NMIM).	

0806 Kawalan Teknikal Keterdedahan (*Vulnerability)*

Objektif:

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

080601 Kawalan dari Ancaman Teknikal

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) memperoleh maklumat teknikal keterdedahan yang terkini ke atas sistem maklumat yang digunakan; b) menilai tahap teknikal keterdedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; c) mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan; d) aktiviti *Security Posture Assessment* perlu dilaksanakan sekurang-kurangnya sekali dalam tempoh dua (2) tahun atau mengikut keperluan; dan e) aset ICT *EOL*, *EOS* atau *BER* yang mendedahkan JPPM kepada risiko keselamatan siber atau mengganggu perkhidmatan hendaklah dikenal pasti dan dikawal bagi meminimumkan risiko.	ICTSO, Pentadbir ICT dan Pihak Ketiga

080602 Perisian dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) hanya perisian yang berlesen dan diperakui sahaja dibenarkan bagi kegunaan JPPM. Warga JPPM tidak dibenarkan memuat turun, membuat instalasi dan mengguna perisian yang boleh mendatangkan kemudaratan serta kerosakan kepada aset ICT dan rangkaian; b) warga JPPM tidak dibenarkan menyebar sebarang perisian berlesen secara tidak sah. JPPM tidak akan bertanggungjawab ke atas sebarang kesalahan yang	ICTSO, Pentadbir ICT dan Warga JPPM

dilakukan oleh warga JPPM;

c) sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Ketua Pengarah JPPM;

d) 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

e) *source code* sesebuah sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

BIDANG 09 KESELAMATAN KOMUNIKASI

0901 Pengurusan Keselamatan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

090101 Kawalan Infrastruktur Rangkaian

Infrastruktur rangkaian mestilah dikawal dan diuruskan dengan baik bagi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.

ICTSO, Pentadbir ICT, Warga JPPM dan Pihak Ketiga

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan akses serta 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) akses kepada peralatan rangkaian hendaklah dikawal dan terhad kepada warga JPPM serta pihak ketiga yang dibenarkan sahaja;
d) semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;
e) *Firewall* dan *Web Application Firewall (WAF)* 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 warga JPPM kecuali mendapat kebenaran ICTSO;

h) memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh serta aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JPPM;

i) sebarang penyambungan rangkaian yang bukan di bawah kawalan JPPM adalah tidak dibenarkan;

j) semua warga JPPM hanya dibenarkan menggunakan rangkaian JPPM sahaja dan penggunaan modem adalah dilarang sama sekali; dan

k) kemudahan bagi *wireless* LAN hendaklah dikawal.

0902 Pengurusan Pemindahan/Pertukaran Maklumat

Objektif:

Memastikan keselamatan pemindahan/pertukaran maklumat antara JPPM dan pihak ketiga terjamin.

090201 Kawalan Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — ICTSO, Pentadbir ICT dan Warga JPPM

a) polisi dan prosedur kawalan pemindahan/pertukaran maklumat perlu diwujudkan untuk melindungi pemindahan/pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;

b) perjanjian perlu diwujudkan untuk pemindahan/pertukaran maklumat di antara JPPM dengan pihak ketiga; dan

c) media yang mengandungi maklumat perlu dilindungi daripada akses yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari JPPM.

090202 Perjanjian Pemindahan/Pertukaran Maklumat

JPPM perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan/pertukaran maklumat antara JPPM dengan pihak ketiga.

CDO, Warga JPPM dan Pihak Ketiga

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) CDO hendaklah mengawal penghantaran dan penerimaan maklumat JPPM;
b) prosedur bagi memastikan tiada gangguan/sangkalan semasa pemindahan data dan maklumat JPPM;
c) mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan
d) JPPM hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.

090203 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.

Warga JPPM

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

a) akaun atau alamat e-mel yang diperuntukkan oleh JPPM sahaja boleh digunakan bagi urusan rasmi Kerajaan;
b) penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
c) warga JPPM dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua puluh lima megabait (25Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;
d) warga JPPM hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;
e) warga JPPM hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;
f) setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;
g) warga JPPM hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan
h) warga JPPM hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.

0903 Perkhidmatan Dalam Talian (*Online)*

Objektif:

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

090301 Kawalan Perkhidmatan Dalam Talian (Online)

Bagi menggalakkan perkhidmatan dalam talian serta sebagai menyokong hasrat Kerajaan mengoptimumkan penyampaian perkhidmatan melalui elektronik, warga JPPM dan pihak ketiga boleh menggunakan kemudahan Internet.

Warga JPPM dan Pihak Ketiga

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) maklumat yang terlibat dengan transaksi dalam talian perlu dilindungi daripada penghantaran yang tidak lengkap, salah destinasi, aktiviti penipuan, pertikaian kontrak dan pendedahan, duplikasi atau pengulangan mesej serta pengubahsuaian yang tidak dibenarkan; dan
b) kerahsiaan dan integriti maklumat yang disediakan untuk sistem yang boleh diakses oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

090302 Maklumat Umum

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan siber adalah seperti berikut:

CDO, ICTSO dan Warga JPPM

a) perisian, data dan maklumat hendaklah dilindungi dengan mekanisme yang bersesuaian;
b) sistem yang boleh diakses oleh orang awam hendaklah diuji terlebih dahulu; dan
c) segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.

0904 Media Sosial

Objektif:

Memastikan keselamatan dan kawalan penyebaran maklumat melalui media sosial.

090401 Kawalan Media Sosial

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi serta disebarkan melalui media sosial adalah seperti berikut:

Warga JPPM

a) tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara;
b) tidak melibatkan penyebaran maklumat dan dokumen rahsia rasmi;
c) tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan;
d) tidak menyentuh isu sensitif seperti agama, politik dan perkauman; dan
e) tidak memaparkan kenyataan yang berunsur fitnah atau hasutan.

Warga JPPM boleh merujuk kepada dokumen Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam oleh MAMPU.

BIDANG 10 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

1001 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:

Memastikan sistem dan aplikasi yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan siber yang bersesuaian serta dikawal dan dikendalikan dengan baik dan selamat.

100101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: — CDO, ICTSO dan Pentadbir ICT

a) perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi mengelakkan sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;
b) aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan
c) semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan kesahihan dan integriti data serta memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.

100102 Keselamatan Persekitaran Pembangunan Sistem

Keselamatan persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem (*development lifecycle*). — ICTSO dan Pentadbir ICT

Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan di JPPM. Perkara-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.

100103 Kawalan Sistem Maklumat dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

ICTSO, Pentadbir ICT dan Pihak Ketiga

a) perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan serta disahkan sebelum diguna pakai;
b) proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;
c) aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian serta pangkalan data untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan JPPM;
d) Pentadbir ICT perlu memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga;
e) mengawal perubahan dan/atau pindaan ke atas pakej perisian serta memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;
f) akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada warga JPPM dan pihak ketiga yang dibenarkan sahaja;
g) pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh Pentadbir ICT.

h) kod sumber (*source code),* data/maklumat, prosedur dan dokumen yang dibangunkan secara *outsource* bagi semua aplikasi dan perisian adalah menjadi hak milik JPPM.

i) menghalang sebarang peluang untuk membocorkan maklumat;

j) kawalan yang bersesuaian dan log audit perlu direka bentuk ke dalam sistem aplikasi.

k) pembangunan sistem hendaklah menggunakan teknik *secure coding*;

l) semua sistem baharu dan penambahbaikan sistem sedia ada hendaklah menjalani ujian penerimaan sistem bagi memastikan garis panduan keselamatan dipenuhi serta lulus *User Acceptance Test (UAT)* dan *Final Acceptance Test (FAT)* sebelum sistem diguna pakai;

m) data ujian perlu dipilih dengan teliti, dilindungi dan dikawal; dan

n) pembangunan sistem atau aplikasi yang melibatkan integrasi dengan sistem induk menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian hendaklah dilindungi daripada risiko ancaman keselamatan.

100104 Prinsip Kejuruteraan Keselamatan Sistem

Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independant Verification and Validation (IV&V)* Sektor Awam yang terkini.

ICTSO dan Pentadbir ICT

100105 Validasi Data *Input* dan *Output*

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Pentadbir ICT

a) data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan adalah betul dan bersesuaian; dan
b) data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

100106 Sekatan Ke Atas Perubahan Dalam Pakej Perisian

Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan serta terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal. Pentadbir ICT

BIDANG 11 HUBUNGAN PEMBEKAL

1101 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal

Objektif:

Memastikan aset ICT JPPM yang boleh diakses oleh pembekal dilindungi.

110101 Keselamatan Maklumat berkaitan Hubungan Pembekal

Strategi mitigasi risiko keselamatan maklumat perlu didokumenkan apabila pembekal dibenarkan untuk akses kepada aset ICT JPPM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) mengenal pasti dan mendokumenkan jenis-jenis pembekal seperti perkhidmatan ICT, logistik, kewangan dan sebagainya; b) mengenal pasti jenis aset ICT yang dibenarkan untuk diakses oleh pembekal serta melakukan pemantauan dan pengawalan terhadap aset tersebut secara berterusan; c) memberi pendedahan terhadap polisi dan prosedur berkaitan keselamatan siber; d) mewujudkan mekanisme/proses pengurusan pembekal dengan mengambil kira aspek keselamatan siber sebagai teras; e) pemantauan berterusan hendaklah dilakukan terhadap semua pembekal dengan melaksanakan pengukuran prestasi dan pematuhan terhadap garis panduan keselamatan siber; f) mewujudkan kontrak rasmi bersama pembekal yang dapat menjamin keselamatan siber JPPM di samping segala urusan bersama pembekal hendaklah dilaksanakan secara	CDO, ICTSO, Pemilik Projek, Pentadbir ICT dan Pembekal

rasmi; dan

g) mewujudkan perjanjian yang jelas agar pihak pembekal memastikan keselamatan maklumat yang digunakan terjamin sepanjang akses dibenarkan dan seterusnya memulangkan kembali akses maklumat sekiranya kontrak mereka tamat atau ditamatkan.

110102 Rangkaian Pembekal ICT

Kandungan perjanjian bersama pembekal hendaklah diwujudkan bagi memastikan risiko keselamatan siber berkaitan rangkaian pembekal khidmat ICT dan produk diambil kira.

CDO, ICTSO, Pentadbir ICT dan Pembekal

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) mengenal pasti keperluan keselamatan siber khusus berkaitan dengan perolehan rangkaian pembekal perkhidmatan dan produk ICT sebagai tambahan kepada keperluan umum keselamatan siber berkaitan hubungan sub-pembekal;
b) rangkaian pembekal yang terlibat dalam menyediakan perkhidmatan dan produk ICT JPPM perlu didedahkan dengan keselamatan siber (polisi, prosedur, proses) berkaitan mengikut setiap aras pembekal termasuklah sub-pembekal atau sub-sub-pembekal;
c) melaksanakan proses pemantauan rangkaian pembekal perkhidmatan dan produk ICT dengan kaedah yang berkesan bagi menjamin keperluan keselamatan siber 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 di kalangan rangkaian pembekal; dan

f) mewujudkan mekanisma khusus untuk mengurus rangkaian pembekal perkhidmatan dan produk ICT bagi memastikan keselamatan siber terjamin. Mekanisme yang diwujudkan wajar mampu untuk mengurus risiko sekiranya komponen produk yang dibekalkan tidak lagi boleh dibekalkan kerana perubahan trend dan teknologi yang berlaku.

1102 Pengurusan Penyampaian Perkhidmatan Pembekal

Objektif:

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan siber serta penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal.

110201 Perkhidmatan Penyampaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: CDO, ICTSO, Pemilik Projek, dan Pembekal

a) kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian hendaklah dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal;

b) perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal 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.

110202 Pemantauan dan Kajian Perkhidmatan Pembekal

JPPM sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) memantau tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan; b) laporan perkhidmatan yang dihasilkan oleh pembekal perlu dipantau dan status kemajuan dikemukakan kepada JPPM; dan c) memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	CDO, ICTSO, Pemilik Projek, dan Pembekal

110203 Pengurusan Perubahan Perkhidmatan Pembekal

Semua perubahan perkhidmatan pembekal dilaksanakan secara teratur dan mengikut klausa kontrak yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) perubahan dalam perjanjian dengan pembekal; b) perubahan yang dilakukan oleh JPPM bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) perubahan dalam perkhidmatan pembekal selaras dengan perubahan-perubahan melibatkan rangkaian, teknologi, produk, perkakasan, lokasi serta pertukaran pembekal dan subkontraktor.	CDO, ICTSO, Pemilik Projek, dan Pembekal

BIDANG 12 PENGURUSAN DAN PENGENDALIAN INSIDEN KESELAMATAN SIBER

1201 Pelaporan Insiden Keselamatan Siber

Objektif:

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

120101 Mekanisme Pelaporan Insiden Keselamatan Siber

Insiden keselamatan siber bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT. Insiden keselamatan siber yang berlaku hendaklah dilaporkan kepada ICTSO/JPPM CSIRT dengan kadar segera.

ICTSO, JPPM CSIRT dan Warga JPPM

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

Pelaporan insiden keselamatan siber di JPPM adalah berdasarkan:

a) Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam; dan
b) Prosedur Operasi Standard: Pengurusan dan Pengendalian Insiden Keselamatan Siber.

1202 Pengurusan Maklumat Insiden Keselamatan Siber

Objektif:

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan siber.

120201 Pengurusan Insiden

Maklumat mengenai insiden keselamatan siber yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. — ICTSO dan JPPM CSIRT

Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada JPPM.

Bahan-bahan bukti berkaitan insiden keselamatan siber disimpan dan diselenggarakan. Prosedur pengurusan insiden perlu diwujudkan dan didokumenkan.

Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah

seperti berikut:

a) mengenal pasti semua jenis insiden keselamatan siber seperti gangguan perkhidmatan yang disengajakan, pemalsuan indentiti dan pengubahsuaian perisian tanpa kebenaran;
b) menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;
c) menyimpan jejak audit, melaksanakan aktiviti penduaan secara berkala dan melindungi integriti semua bahan bukti;
d) menyediakan pelan tindakan pemulihan segera; dan
e) memaklumkan atau mendapatkan nasihat pihak berkuasa/perundangan sekiranya perlu.

120202 Penilaian dan Keputusan Terhadap Insiden Keselamatan Siber

Insiden keselamatan siber hendaklah dinilai dan keputusan perlu dibuat jika insiden tersebut diklasifikasikan sebagai insiden keselamatan siber. — ICTSO dan JPPM CSIRT

Perkara-perkara yang perlu diambil kira dalam penilaian insiden keselamatan siber adalah seperti berikut:

a) penilaian perlu dibuat berdasarkan klasifikasi insiden yang dipersetujui;
b) insiden perlu disusun mengikut kepentingan dan implikasi kepada JPPM;
c) hasil daripada penilaian yang dibuat boleh dipanjangkan kepada pihak berkuasa supaya pengesahan atau penilaian semula dapat dilakukan; dan
d) hasil daripada penilaian juga perlu direkodkan dengan terperinci untuk rujukan masa depan dan verifikasi.

120203 Tindak balas Terhadap Insiden Keselamatan Siber

Insiden keselamatan siber hendaklah ditangani sewajarnya oleh pihak yang bertanggungjawab mengikut prosedur yang berkaitan. Matlamat utama tindak balas terhadap insiden keselamatan siber adalah untuk mengembalikan tahap keselamatan ke paras normal dan seterusnya melaksanakan langkah-langkah pemulihan sewajarnya berdasarkan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT JPPM.	ICTSO dan JPPM CSIRT

BIDANG 13 KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1301 Dasar Kesinambungan Perkhidmatan

Objektif:

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

130101 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan (PKP) JPPM hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan.

Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan JPPM.

CDO, ICTSO, Pasukan Pemulihan Bencana JPPM dan Pihak Ketiga

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 siber;
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 warga JPPM mengenai prosedur kecemasan;

f) merekod maklumat bagi *backup* termasuklah lokasi sebenar penyimpanannya, arahan pemulihan maklumat dan kemudahan yang berkaitan; dan
g) menguji dan mengkaji semula pelan sekurang-kurangnya setahun sekali.

PKP JPPM hendaklah mengandungi perkara-perkara berikut:

a) senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b) senarai warga JPPM dan pihak pembekal yang berkaitan berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai pengganti juga disediakan sebagai menggantikan pihak yang tidak dapat hadir untuk menangani insiden;
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 PKP JPPM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. PKP JPPM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian PKP JPPM hendaklah dijadualkan untuk memastikan

semua ahli yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

JPPM hendaklah memastikan salinan PKP sentiasa dikemaskini dan diberikan perlindungan yang sama seperti di lokasi utama.

130102 Mengesah, Mengkaji Semula dan Menilai Keselamatan Maklumat Dalam Pelan Pengurusan Kesinambungan Perkhidmatan

JPPM mengesahkan terdapat kawalan terhadap keselamatan siber dalam PKP JPPM. Semakan kesinambungan kawalan keselamatan dikaji semula secara berkala dan apabila berlaku perubahan kepada peraturan yang sedang berkuat kuasa untuk memastikan pelan berkenaan sahih dan berkesan semasa berlaku gangguan/bencana.	CDO, ICTSO, Pasukan Pemulihan Bencana JPPM dan Pihak Ketiga

1302 Lewahan (*Redundancy)*

Objektif:
Untuk memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.

130201 Kebolehsediaan Fasiliti Pemprosesan Maklumat

Kemudahan pemprosesan maklumat JPPM perlu mempunyai lewahan (*redundancy*) yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan tersebut perlu diuji (*failover test*) keberkesanannya dari semasa ke semasa.	CDO, ICTSO, Pentadbir ICT dan Pemilik Projek

Untuk tujuan itu, perkara-perkara berikut wajar diberi tumpuan:

a) JPPM perlu mengenal pasti 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 lewahan fasiliti pemprosesan perlu dipertimbangkan;

c) fasiliti pemprosesan tersebut perlu diuji bagi memastikan kesiapsediaan menjalankan operasi apabila fasiliti pemprosesan utama gagal berfungsi; dan

d) kewujudan lewahan fasiliti pemprosesan boleh membawa kepada risiko kewibawaan dan kerahsiaan maklumat dan sistem maklumat. Hal ini perlu diambil kira semasa sesuatu sistem maklumat itu dibangunkan.

BIDANG 14 PEMATUHAN

1401 Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan dan memantapkan tahap keselamatan siber bagi mengelak dari pelanggaran kepada undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat dan PKS JPPM.

140101 Pematuhan Dasar

Semua warga JPPM dan pihak ketiga hendaklah membaca, memahami dan mematuhi PKS JPPM serta undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.	Warga JPPM dan Pihak Ketiga
Semua aset ICT di JPPM termasuk maklumat yang disimpan di dalamnya adalah hak milik JPPM dan JPPM berhak untuk memantau aktiviti warga JPPM serta pihak ketiga untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Pihak JPPM berhak tidak memberikan kemudahan ICT jika pematuhan dasar tidak diperakui secara rasmi oleh warga JPPM dan pihak ketiga.	
Sebarang penggunaan aset ICT JPPM selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalangunaan sumber JPPM.	

140102 Pematuhan Dasar dan Piawaian bagi Keperluan Teknikal

ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.	ICTSO dan Pentadbir ICT

Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan siber.

140103 Pematuhan Keperluan Audit

Pematuhan kepada keperluan audit adalah 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. Akses ke atas maklumat bagi tujuan pengauditan perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Warga JPPM

140104 Keperluan Perundangan

Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga JPPM adalah seperti di **Lampiran 1.**	Warga JPPM

140105 Pelanggaran Dasar

Sebarang pelanggaran dasar dan peraturan oleh warga JPPM akan dikenakan tindakan tertakluk kepada undang-undang dan peraturan yang sedang berkuatkuasa. Sebarang aduan tentang pelanggaran dasar hendaklah dibuat secara bertulis kepada CDO. CDO boleh melantik jawatankuasa untuk menyiasat, meneliti laporan dan membuat keputusan sekiranya siasatan terperinci perlu dilaksanakan.	Warga JPPM

140106 Hak Harta Intelek (*Intellectual Property Rights* – IPR)

Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelek. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Warga JPPM dan Pihak Ketiga

1402 Kajian Semula Keselamatan Maklumat

Objektif:

Memastikan keselamatan siber dilaksanakan mengikut polisi dan prosedur JPPM.

140201 Kajian Semula Keselamatan Maklumat Secara Berkecuali

Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur ICT.	ICTSO

140202 Pematuhan Polisi dan Standard Keselamatan

JPPM hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat serta prosedur di kawasan yang dipertanggungjawabkan dengan polisi, standard termasuklah keperluan teknikal yang bersesuaian.	ICTSO

140203 Kajian Semula Pematuhan Teknikal

JPPM hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung dalam polisi, standard dan keperluan komputer.	JPICT dan ICTSO

LAMPIRAN 1

SENARAI PERUNDANGAN DAN PERATURAN

1) Akta Rahsia Rasmi 1972;
2) Akta Tandatangan Digital 1997;
3) Akta Jenayah Komputer 1997;
4) Akta Hak Cipta (Pindaan) 2022;
5) Akta Komunikasi dan Multimedia 1998;
6) Akta Pertubuhan 1966;
7) Akta Pencegahan Dan Pengawalan Penyakit Berjangkit 1988;
8) Akta Perbendaharaan;
9) Arahan Keselamatan;
10) Arahan Pendaftar Pertubuhan;
11) Arahan Teknologi Maklumat 2007;
12) Perintah-Perintah Am;
13) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA);
14) 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;
15) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
16) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
17) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.
18) Surat Arahan MAMPU. BDPICT (S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk “Penggunaan Media Jaringan Sosial di Sektor Awam”;
19) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
20) Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam;

21) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
22) Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
23) Surat Pemakluman Kaedah Pelaksanaan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 6 April 2022;
24) Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019;
25) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
26) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
27) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
28) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam;
29) Pekeliling Perkhidmatan Bil 5 2007 bertajuk “Panduan Pengurusan Pejabat”;
30) Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)]
31) Portal Pekeliling Perbendaharaan (PPP) – Tatacara Pengurusan Aset Alih Kerajaan;
32) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
33) Peraturan-Peraturan Pencegahan Dan Pengawalan Penyakit Berjangkit (Pengkompaunan Kesalahan-Kesalahan) (Pindaan) (No.7) 2020;
34) Peraturan-Peraturan Pencegahan Dan Pengawalan Penyakit Berjangkit (Langkah-Langkah Di Dalam Kawasan Tempatan Jangkitan) (No.7) 2020;
35) Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan ISO/IEC 27001:2013 dalam Sektor Awam
36) Pelan Kesinambungan Perkhidmatan (PKP) JPPM;
37) *Standard Operating Procedure* (SOP) dan Prosedur ICT JPPM.