DASAR KESELAMATAN ICT

JABATAN BOMBA DAN PENYELAMAT MALAYSIA (JBPM)

RUJUKAN	VERSI	TARIKH	BIL. M/SURAT
DKICT JBPM	VERSI 1.3	1 OGOS 2015	43

DASAR KESELAMATAN ICT

JABATAN BOMBA DAN PENYELAMAT MALAYSIA (JBPM)

SEJARAH DOKUMEN

RUJUKAN	VERSI	TARIKH	BIL. M/SURAT
DKICT JBPM	VERSI 1.0	01 OKTOBER 2009	42
DKICT JBPM	VERSI 1.1	16 MAC 2011	42
DKICT JBPM	VERSI 1.2	12 DISEMBER 2013	42
DKICT JBPM	VERSI 1.3	1 OGOS 2015	43

JADUAL PERKARA PINDAAN
DASAR KESELAMATAN ICT JBPM

Bil	Versi 1.2	Versi 1.3
1.	*Perkara : 040201 Pelaporan Insiden* *Nota 2 :* Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT" mengenainya bolehlah dirujuk. *Muka surat 15*	Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT" dan Surat Pekeliling Am Bil. 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam" mengenainya bolehlah dirujuk.
2.	*Perkara : 090101 Pelan Kesinambungan Perkhidmatan* *Tanggungjawab : ICTSO* *Muka surat 35*	CIO, Pengurus ICT, ICTSO, Pentadbir Sistem
3.	*Perkara : 09 Pengurusan Kesinambungan Perkhidmatan* *Dasar Kesinambungan Perkhidmatan* *Penambahan perkara 090102, perkara 091203 dan perkara 090104* *Muka surat 35*	**090102 Pelan Pemulihan Bencana** Pelan pemulihan bencana *atau disaster recovery plan* (DRP) hendaklah dibangunkan sebagai sebahagian daripada pelan kesinambungan perkhidmatan. Pelan pemulihan bencana atau *disaster recovery plan* (DRP) adalah untuk memastikan perkhidmatan dan operasi sistem aplikasi yang kritikal dapat diteruskan sekiranya berlaku bencana ke atas kemudahan atau infrastruktur, perkakasan dan perisian utama bagi perkhidmatan yang tersebut. **090103 Pelan Pengurusan Pemulihan Bencana** Pelan pengurusan pemulihan bencana atau *disaster recovery management plan* (DRMP) mestilah mengandungi sekurang-kurangnya perkara-perkara yang berikut : a. Skop pelan pemulihan bencana; b. Definisi bencana dan andaian bagi pelaksanaan pelan pemulihan bencana; c. Dasar dan piawaian berkaitan;

Bil	Versi 1.2	Versi 1.3
		d. Strategi pemulihan bencana; e. Struktur pasukan pemulihan bencana atau *disaster recovery team* (DRT); f. Carta aliran proses pemulihan bencana; g. Prosedur sebelum bencana; h. Prosedur semasa bencana; i. Prosedur selepas bencana; dan j. Penilaian semula bencana. **090104 Pelan Teknikal Pemulihan Bencana** Pelan teknikal pemulihan bencana atau *disaster recovery technical plan* (DRTP) mestilah mengandungi sekurang-kurangnya perkara-perkara yang berikut : a. Senarai dan maklumat perhubungan yang diperlukan semasa berlaku kecemasan akibat bencana; b. Maklumat oerganisasi Cawangan Teknologi Maklumat (CTM); c. Senarai sistem aplikasi kritikal; d. Maklumat penting pusat data utama atau *production data centre*; e. Maklumat penting pusat pemulihan bencana atau *disaster recovery centre;* f. Maklumat organisasi pasukan pemulihan bencana atau disaster recovery team (DRT); g. Peranan dan tanggungjawab setiap ahli pasukan pemulihan bencana; h. Strategi pemulihan ICT; dan i. Prosedur pemulihan sistem aplikasi kritikal.
4.	*Perkara : 100102 Keperluan Perundangan* (Penambahan pekeliling dan garis panduan dari masa ke masa) *Muka surat 38*	1. Surat Arahan Ketua Setiausaha Negara : Langkah-Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-Lain Peralatan Komunikasi ICT Tanpa Kebenaran (Tarikh : 31 Januari 2007) 2. Etika Penggunaan Media Sosial Dalam Sektor Awam terbitan MAMPU. (2015)

KANDUNGAN

DASAR KESELAMATAN ICT JBPM

PENGENALAN

Dasar Keselamatan ICT (DKICT) Jabatan Bomba dan Penyelamat Malaysia mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) JBPM. Dasar ini juga menerangkan kepada semua pengguna di JBPM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT JBPM.

OBJEKTIF

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

Objektif utama Dasar Keselamatan ICT JBPM ialah seperti berikut:

a) Memastikan kelancaran operasi JBPM dan meminimumkan kerosakan atau kemusnahan.

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

c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN DASAR

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

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

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

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

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

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

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

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

(b) Integriti – Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(c) Tidak Boleh Disangkal – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

(d) Kesahihan – Data dan maklumat hendaklah dijamin kesahihannya; dan

(e) Ketersediaan – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

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

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

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

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT JBPM merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan JBPM. 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 JBPM;

(c) Perkhidmatan

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

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) Data atau Maklumat

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

(e) Manusia

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

(f) Premis Komputer Dan Komunikasi

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

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT JBPM dan perlu dipatuhi adalah seperti berikut:

a. Akses atas dasar perlu mengetahui

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

b. Hak akses minimum

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

c. Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT JBPM;

d. Pengasingan

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

e. Pengauditan

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

f. Pematuhan

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

g. Pemulihan

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

h. Saling Bergantungan

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

Perkara 01 Pembangunan dan Penyelenggaraan Dasar

Dasar Keselamatan ICT		
Objektif : DKICT JBPM diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran operasi jabatan secara berterusan, meminimumkan kerosakan atau kemusnahan aset-aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan.		
010101 Pelaksanaan Dasar		
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah JBPM dibantu oleh Jawatankuasa Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), semua Penolong Ketua Pengarah dan Pengarah Bahagian.	Ketua Pengarah
010102 Penyebaran Dasar		
	Dasar ini perlu disebarkan kepada semua pengguna JBPM (termasuk kakitangan, pembekal, pakar runding dll.)	ICTSO
010103 Penyelenggaraan Dasar		
	Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT JBPM: a. kenal pasti dan tentukan perubahan yang diperlukan; b. kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatan Kuasa Keselamatan ICT (JKICT); c. perubahan yang telah dipersetujui oleh JKICT dimaklumkan kepada semua pengguna; dan d. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	ICTSO
010104 Pengecualian Dasar		
	Dasar Keselamatan ICT JBPM adalah terpakai kepada semua pengguna ICT JBPM dan tiada pengecualian diberikan.	Semua

Perkara 02 Organisasi Keselamatan

Infrastruktur Organisasi Keselamatan		
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.		
020101 Ketua Pengarah		
	Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: a. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT JBPM; b. memastikan semua pengguna mematuhi Dasar Keselamatan ICT JBPM; c. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; d. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT JBPM.	Ketua Pengarah
020102 Ketua Pegawai Maklumat (CIO)		
	Timbalan Ketua Pengarah (P) JBPM adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut: a. membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. menentukan keperluan keselamatan ICT; dan c. membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.	CIO
020103 Pegawai Keselamatan ICT (ICTSO)		
	Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut; a. mengurus keseluruhan program-program keselamatan ICT JBPM;	ICTSO

	b. menguatkuasakan Dasar Keselamatan ICT JBPM; c. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT JBPM kepada semua pengguna. d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT JBPM. e. Menjalankan pengurusan risiko; f. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah - langkah perlindungan yang bersesuaian; h. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO; i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal plasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT JBPM; dan k. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
020104 Pengurus ICT		
	Ketua Penolong Pengarah Cawangan Teknologi Maklumat (CTM) adalah merupakan Pengurus ICT JBPM. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut; a. membaca, memahami dan mematuhi Dasar Keselamatan ICT JBPM; b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan JBPM; c. menentukan kawalan akses semua pengguna terhadap aset ICT JBPM;	Pengurus ICT

	d. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan e. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT JBPM.	
020105 Pentadbir Sistem ICT		
	Pegawai Teknologi Maklumat di Cawangan Teknologi Maklumat JBPM adalah merupakan Pentadbir Sistem ICT JBPM. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT JBPM; c. memantau aktiviti capaian harian pengguna; d. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. menyimpan dan menganalisis rekod jejak audit; dan f. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	CTM
020106 Pengguna		
	Peranan dan tanggungjawab pengguna adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT JBPM; b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. lulus tapisan keselamatan; d. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat JBPM; e. melaksanakan langkah-langkah perlindungan seperti	Pengguna

	berikut: i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. menentukan maklumat sedia untuk digunakan; iv. menjaga kerahsiaan kata laluan; v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g. menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. menandatangani "Surat Akuan Pematuhan" Dasar Keselamatan ICT JBPM.	
Pihak Ketiga		
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.		
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga		
	Akses kepada aset ICT JBPM perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterikan: a. Dasar Keselamatan ICT JBPM; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; d. Hak Harta Intelek;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

	Nota 1: Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk “Tatacara Penyediaan, Penilaian dan Penerimaan Tender” dan Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk “Peraturan Perolehan Perkhidmatan Perundingan” yang berkaitan juga boleh dirujuk.	

Perkara 03 Kawalan dan Pengelasan Aset

Akauntabiliti Aset		
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JBPM.		
030101 Inventori Aset		
	Semua aset ICT JBPM hendaklah direkodkan. Ini termasuklah mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem Semua
Pengelasan dan Pengendalian Maklumat		
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
030201 Pengelasan Maklumat		
	Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut : a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad	Semua
030202 Pengendalian Maklumat		
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. menentukan maklumat sedia untuk digunakan;	Semua

	d. menjaga kerahsiaan kata laluan; e. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. memberi perhatian kepada maklumat terperingkat penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

Perkara 04 Keselamatan Sumber Manusia

Keselamatan Sumber Manusia		
Objektif: Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT JBPM.		
040101 Tanggungjawab Keselamatan		
	Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, di rekod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	Semua
040102 Terma dan Syarat Perkhidmatan		
	Semua warga JBPM yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	Semua
040103 Perakuan Akta Rahsia Rasmi		
	Warga JBPM yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua
Menangani Insiden Keselamatan ICT		
Objektif: Meminimumkan kesan insiden keselamatan ICT.		
040201 Pelaporan Insiden		
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: a. maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau,disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;	Semua

	d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Nota 2: *Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT"* dan *Surat Pekeliling Am Bil. 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam"* mengenainya bolehlah dirujuk.	
Pendidikan		
Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.		
040301 Program Kesedaran Keselamatan ICT		
	Setiap pengguna di JBPM perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT JBPM.	ICTSO
Tindakan Tatatertib		
Objektif: Meningkatkan kesedaran dan pematuhan ke atas Dasar Keselamatan ICT JBPM.		
040401 Pelanggaran Dasar		
	Pelanggaran Dasar Keselamatan ICT JBPM boleh dikenakan tindakan tatatertib.	Semua

Perkara 05 Keselamatan Fizikal

Keselamatan Kawasan		
Objektif: Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.		
050101 Perimeter Keselamatan Fizikal		
	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut: a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memperkukuhkan dinding dan siling; d. Memasang alat penggera atau kamera; e. Menghadkan jalan keluar masuk; f. Mengadakan kaunter kawalan; g. Menyediakan tempat atau bilik khas untuk pelawat-pelawat ; dan h. Mewujudkan perkhidmatan kawalan keselamatan.	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO
050102 Kawalan Masuk Fizikal		
	a. Setiap pengguna JBPM hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara; d. Kehilangan pas mestilah dilaporkan dengan segera;	Semua dan pelawat

	e. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT JBPM.	
050103 Kawasan Larangan		
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dlaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di JBPM adalah bilik Ketua Pengarah, bilik-bilik Timbalan Ketua Pengarah, bilik Server dan bilik-bilik yang diisytiharkan sebagai kawasan larangan. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja: a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu; b. Pihak Ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan c. Semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rahsia hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	Semua
Keselamatan Peralatan		
Objektif: Melindungi peralatan dan maklumat		
050201 Perkakasan		
	Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu: a. Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna; b. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai cirri-ciri keselamatan; c. Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan d. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO.	Semua

050202 Dokumen		
	Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a. memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; c. menggunakan penyulitan *(encryption)* ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan d. memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak.	Semua
050203 Media Storan		
	Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat: a. penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan d. pergerakan media storan hendaklah direkodkan.	Semua
050204 Kabel		
	Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan	CTM dan ICTSO

	c. Melindungi laluan pemasangan kabel sepenuhnya.	
050205 Penyelenggaraan		
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti: a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan d. Semua penyelenggaraan mestilah mendapat kebenaran daripada Penolong Ketua Pengarah atau Pengarah Bahagian berkenaan.	Semua
050206 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat		
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan: a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Semua
050207 Peralatan Di Luar Premis		
	Bagi perkakasan yang dibawa keluar dari premis JBPM, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawasan JBPM; a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambil kira cirri-ciri keselamatan yang bersesuaian.	Semua
050208 Pelupusan		
	Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan JBPM:	Semua

	a. Semua kandungan peralatan khusunya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan c. Maklumat lanjut pelupusan bolehlah merujuk kepada surat pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk ”Garis Panduan Pelupusan Peralatan Komputer ‘’	
050209 *Clear Desk* dan *Clear Screen*		
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja warga atau di paparan skrin apabila warga tidak berada di tempatnya: a. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; b. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci.	Semua
Keselamatan Persekitaran		
Objektif: Melindungi aset ICT JBPM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		
050301 Kawalan Persekitaran		
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis samada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil : a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;	Semua

	c. Peralatan Perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
050302 Bekalan Kuasa		
	a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti UPS *(Uninterrupable Power System)* 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.	CTM, ICTSO

Perkara 06 Pengurusan Operasi Dan Komunikasi

Pengurusan Prosedur Operasi		
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.		
060101 Pengendalian Prosedur		
	a. Semua prosedur keselamatan ICT yang diwujud, dikenalpasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Semua
060102 Kawalan Perubahan		
	a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan 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 ataupun tidak.	Semua
060103 Prosedur Pengurusan Insiden		
	Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut; a. Mengenalpasti semua jenis insiden keselamatan ICT	JPICT KPKT, ICTSO

	seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. Menyimpan jejak audit dan memelihara bahan bukti; dan d. Menyediakan tindakan pemulihan segera.	
Perancangan dan Penerimaan Sistem		
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
060201 Perancangan Kapasiti		
	a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. Keperluan kapasiti ini juga perlu mengambilkira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT, ICTSO
060202 Penerimaan Sistem		
	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT, ICTSO
Perisian Berbahaya		
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan.		
060301 Perlindungan dari Perisian Berbahaya		
	a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan *Instrusion Detection System* (IDS) dan mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;	Semua

	d. Mengemaskini *pattern* anti virus berdasarkan kepada *pattern* terkini yang dikeluarkan oleh makmal pembangun perisian antivirus; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
Housekeeping		
Objektif: Melindungi intergriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.		
060401 Penduaan		
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan di *off site.* a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi baru; b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	Semua
060402 Sistem Log		
	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	CTM

	mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	
Pengurusan Rangkaian		
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
060501 Kawalan Infrustruktur Rangkaian		
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan; a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan mestilah melalui proses *Factory Acceptance Check (FAC)* semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh Pentadbir Sistem; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JBPM; g. Semua perisian *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS)* bagi mengesan dan melindungi rangkaian daripada sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JBPM; i. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk ‘’Garis Panduan	CTM

	Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan ‘’ ; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan JBPM hendaklah mendapat kebenaran ICTSO; k. Semua pengguna hanya dibenarkan menggunakan rangkaian JBPM sahaja. Penggunaan modem adalah dilarang sama sekali. Walaubagaimanapun, penggunaan modem sambungan ke internet yang dilanggan oleh Jabatan adalah dibenarkan bagi tujuan rasmi luar pejabat, tertakluk kepada kebenaran CIO Jabatan; dan l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
Pengurusan Media		
Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.		
060601 Penghantaran Dan Pemindahan		
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua
060602 Prosedur Pengendalian Media		
	a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	Semua
060603 Keselamatan Sistem Dokumentasi		
	a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;	Pentadbir Sistem ICT, ICTSO

	b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	
Keselamatan Komunikasi		
Objektif: Melindungi aset ICT melalui sistem komunikasi yang selamat.		
060701 Internet		
	a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan; b. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak terperlihara; e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh JBPM: f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan g. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.	Semua
060702 Mel Elektronik		
	a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh JBPM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh JBPM;	Semua

	c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh (10) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mail; h. Setiap e-mail rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan k. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.	

Perkara 07 Kawalan Capaian

Dasar Kawalan Capaian		
Objektif: Memahami dan mematuhi keselamatan dalam mencapai dan menggunakan aset ICT JBPM.		
070101 Keperluan Dasar		
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada.	CTM, ICTSO
Pengurusan Capaian Pengguna		
Objektif : Mengawal capaian pengguna ke atas aset ICT JBPM		
070201 Akaun Pengguna		
	Pengguna hendaklah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik; c. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu. ii. Bertukar bidang tugas kerja;	Semua

	iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
070202 Jejak Audit		
	Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi: a. maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b. aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan c. maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT
070203 Hak Capaian		
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Semua
070204 Pengurusan Kata Laluan		
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JBPM seperti berikut :- a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik);	Semua

	d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan i. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan.	
Kawalan Capaian Sistem dan Aplikasi		
Objektif : Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.		
070301 Sistem Maklumat dan Aplikasi		
	Capaian sistem dan aplikasi di JBPM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktivii yang tidak diingini; c. Memaparkan notis amaran pada skrin computer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; e. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan cirri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan	Pentadbir Sistem ICT, ICTSO

	f. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
Peralatan Komputer Mudah Alih		
Objektif: Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.		
070401 Penggunaan Peralatan Komputer Mudah Alih		
	a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan ataupun kerosakan; dan b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua

Perkara 08 Pembangunan dan Penyelenggaraan Sistem

Keselamatan Dalam Membangunkan Sistem dan Aplikasi		
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian		
080101 Keperluan Keselamatan		
	a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh menganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; dan c. Sebaik-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik sistem, Pentadbir Sistem ICT, ICTSO
080102 Pengesahan Data Input		
	Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Pentadbir Sistem ICT
080103 Kawalan Prosesan		
	Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem ICT
080104 Pengesahan Data Output		
	Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem ICT
Kriptografi		
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
080201 Penyulitan		
	Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua

080202 Tandatangan Digital		
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
080203 Pengurusan Infrastruktur Kunci Awam (PKI)		
	Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
Fail Sistem		
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		
080301 Kawalan Fail Sistem		
	Fail sistem perlu dikawal dan dikendalikan dengan baik dan selamat. a. Proses pengemas kini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT
Pembangunan dan Proses Sokongan		
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi		
080401 Kawalan Perubahan		
	Perubahan atau pengubah suaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Pentadbir Sistem ICT

Perkara 09 Pengurusan Kesinambungan Perkhidmatan

Dasar Kesinambungan Perkhidmatan		
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
090101 Pelan Kesinambungan Perkhidmatan		
	Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian: a. mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. melaksanakan prosedur–prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. mendokumentasikan proses dan prosedur yang telah dipersetujui; d. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; e. membuat penduaan; dan f. menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	CIO, Pengurus ICT, ICTSO, Pentadbir Sistem
090102 Pelan Pemulihan Bencana		
	Pelan pemulihan bencana atau disaster recovery plan (DRP) hendaklah dibangunkan sebagai sebahagian daripada pelan kesinambungan perkhidmatan. Pelan pemulihan bencana atau disaster recovery plan (DRP) adalah untuk memastikan perkhidmatan dan operasi sistem aplikasi yang kritikal dapat diteruskan sekiranya berlaku bencana ke atas kemudahan atau infrastruktur, perkakasan dan perisian utama bagi perkhidmatan yang tersebut.	CIO, Pengurus ICT, ICTSO, Pentadbir Sistem
090103 Pelan Pengurusan Pemulihan Bencana		
	Pelan pengurusan pemulihan bencana atau *disaster recovery management plan* (DRMP) mestilah mengandungi sekurang-kurangnya perkara-perkara yang berikut :	CIO, Pengurus ICT, ICTSO,

	a. Skop pelan pemulihan bencana; b. Definisi bencana dan andaian bagi pelaksanaan pelan pemulihan bencana; c. Dasar dan piawaian berkaitan; d. Strategi pemulihan bencana; e. Struktur pasukan pemulihan bencana atau *disaster recovery team* (DRT); f. Carta aliran proses pemulihan bencana; g. Prosedur sebelum bencana; h. Prosedur semasa bencana; i. Prosedur selepas bencana; dan j. Penilaian semula bencana. Nota 3 : *Dokumen Pelan Pengurusan Pemulihan Bencana JBPM bolehlah diurjuk.*	Pentadbir Sistem
090104 Pelan Teknikal Pemulihan Bencana		
	Pelan teknikal pemulihan bencana atau *disaster recovery technical plan* (DRTP) mestilah mengandungi sekurang-kurangnya perkara-perkara yang berikut : a. Senarai dan maklumat perhubungan yang diperlukan semasa berlaku kecemasan akibat bencana; b. Maklumat oerganisasi Cawangan Teknologi Maklumat (CTM); c. Senarai sistem aplikasi kritikal; d. Maklumat penting pusat data utama atau *production data centre*; e. Maklumat penting pusat pemulihan bencana atau *disaster recovery centre;* f. Maklumat organisasi pasukan pemulihan bencana atau disaster recovery team (DRT); g. Peranan dan tanggungjawab setiap ahli pasukan pemulihan bencana; h. Strategi pemulihan ICT; dan i. Prosedur pemulihan sistem aplikasi kritikal. Nota 4 : *Dokumen Pelan Teknikal Pemulihan Bencana JBPM bolehlah diurjuk.*	CIO, Pengurus ICT, ICTSO, Pentadbir Sistem

Perkara 10 Pematuhan

Pematuhan dan Keperluan Perundangan		
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT JBPM.		
100101 Pematuhan Dasar		
	Setiap pengguna di JBPM hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT JBPM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di JBPM termasuk maklumat yang disimpan di dalamnya adalah hak milik kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua
100102 Keperluan Perundangan		
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JBPM: 1. Arahan Keselamatan; 2. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”; 3. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); 4. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)”; 5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Me Elektronik di Agensi-agensi Kerajaan”; 6. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; 7. Surat Pekeliling Am Bil. 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam”: 8. Surat Pekeliling Perbendaharaan Bil. 2/1995 (Tambahan Pertama) – “ Tatacara Penyediaan, Penilaian dan	Semua

	Penerimaan Tender"; 9. Surat Pekeliling Perbendaharaan Bil. 3/1995 – "Peraturan Perolehan Perkhidmatan Perundingan"; 10. Akta Tandatangan Digital 1997; 11. Akta Rahsia Rasmi 1972: 12. Akta Jenayah Komputer 1997; 13. Akta Hak cipta (Pindaan) Tahun 1997; 14. Akta Komunikasi dan Multimedia 1998: 15. Perintah – Perintah Am; 16. Arahan Perbendaharaan; dan 17. Arahan Teknologi Maklumat 2007 18. Surat Arahan Ketua Setiausaha Negara : Langkah-Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-Lain Peralatan Komunikasi ICT Tanpa Kebenaran (Tarikh : 31 Januari 2007) 19. Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan. (Tarikh : 1 Jun 2007) 20. Surat Arahan Ketua Pengarah MAMPU : Penggunaan Media Jaringan Sosial Di Sektor Awam. (Tarikh : 19 November 2009) 21. Surat Arahan Ketua Pengarah MAMPU : Panduan_Penyediaan_Berita_Online Dan Penyiaran 22. Berita Online Di Laman Web/Portal Agensi-Agensi Kerajaan. (Tarikh : 11 September 2009) 23. Surat Arahan Ketua Pengarah MAMPU : Garis Panduan Pembangunan Kandungan Sektor Awam. (Tarikh : 11 September 2009) 24. Garis Panduan Pelaksanaan Blog Bagi Agensi Sektor Awam / (Dokumen - Zip Fail) (Tarikh : 17 Julai 2009) 25. Surat Arahan Ketua Pengarah MAMPU Berkaitan Pengaktifan Fail Log Server. (Tarikh : 23 Mac 2009) 26. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem Ict Sektor Awam (Tarikh : 17 November 2009) 27. Surat Arahan Ketua Pengarah MAMPU – Garis Panduan	

	Transisi IPv6 Sektor Awam (Tarikh : 4 Januari 2010) 28. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam (Tarikh : 22 Januari 2010) 29. Surat Arahan Ketua Pengarah MAMPU – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam (Tarikh : 5 Mac 2010) 30. Surat Arahan Ketua Pengarah MAMPU – Pemantapan Penggunaan Dan Pengurusan E-Mel Di Agensi-Agensi Kerajaan (Tarikh : 1 Julai 2010) 31. Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam. (Tarikh : 3 Ogos 2010) 32. Surat Arahan Ketua Pengarah MAMPU : Amalan Terbaik Penggunaan Media Jaringan Sosial. (Tarikh : 8 April 2011) 33. Garis Panduan Penggunaan Perkhidmatan *Wireless Broadband Internet* Dan Media Jaringan Sosial Di Jabatan Bomba Dan Penyelamat Malaysia (JBPM). (Tarikh : 1 Ogos 2012) 34. Etika Penggunaan Media Sosial Dalam Sektor Awam terbitan MAMPU. (2015)	

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk komputer, media storan, *server, router, firewall,* rangkaian dan lain-lain.
Backup	Proses penduaan sesuatu dokumen atau maklumat
Bandwidth	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi
Data center	Pusat simpanan data
Denial of Service	Halangan pemberian perkhidmatan
Downloading	Aktiviti muat-turun sesuatu perisian
Encryption	Enkripsi atau penyulitan. Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecauli penerima yang sah.
Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat *(information theft / espionage)*, penipuan *(hoaxes).*
GCERT	*Government Computer Emergency Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
Hub	Hab 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 Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Insiden Keselamatan	Musibah *(adverse event)* yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut
Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan 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 Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindakbalas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Log out	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse*, *worm, spyware* dan sebagainya.

MODEM	MOodulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui. Maklumat yang diproses dan diperolehi di luar daripada sesuatu organisasi atau struktur kerja.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.
Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access / Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.

Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi
WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.
Worm	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT JBPM

Nama (Huruf Besar) : _____

No. Kad Pengenalan : _____

Jawatan : _____

Bahagian/Jabatan : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT JBPM ; dan

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

…… ……..

(Tanda Tangan Pegawai) Tarikh

Pengesahan Pegawai Keselamatan ICT

…… ……..

(Nama Pegawai Keselamatan ICT) Tarikh

b.p Ketua Pengarah
Jabatan Bomba dan Penyelamat Malaysia