Panduan Keselamatan ICT

Jabatan Tenaga Manusia
Kementerian Sumber Manusia

Versi 1.0

KANDUNGAN

PENGENALAN

Panduan Keselamatan ICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) JTM. Panduan ini juga menerangkan kepada semua pengguna di JTM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT JTM.

OBJEKTIF

Panduan Keselamatan ICT JTM diwujudkan untuk menjamin kesinambungan urusan JTM dengan meminimumkan kesan insiden keselamatan ICT.

SKOP

Panduan Keselamatan ICT MAMPU meliputi aset ICT yang berikut :-

Data dan maklumat – Semua data dan maklumat yang disimpan atau digunakan dipelbagai media atau peralatan ICT;

Peralatan ICT – Semua peralatan komputer dan periferal seperti komputer peribadi, stesen kerja, kerangka utama dan alat-alat prasarana seperti *Uninterrupted Power Supply* (UPS), punca kuasa dan penghawa dingin;

Media Storan – Semua media storan dan peralatan yang berkaitan seperti disket, kartrij, CD-ROM, pita, cakera, pemacu cakera dan pemacu pita dan lain-lain;

Komunikasi dan Peralatan Rangkaian – Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *switch*, *gateway*, *bridge*, *router*, peralatan PABX dan lain-lain;

Perisian – Semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan mengirim maklumat seperti perisian sistem, perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data, fail program, fail data dan lain-lain;

Dokumentasi – Semua dokumentasi yang mengandungi maklumat berkaitan dengan penggunaan dan pemasangan peralatan dan perisian. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, *transparencies*, risalah dan *slides*;

Manusia – Semua pengguna yang dibenarkan termasuk pentadbir dan personel yang bertanggungjawab terhadap keselamatan ICT; dan

Premis Komputer dan Komunikasi – Semua kemudahan serta premis yang diguna untuk menempatkan perkara-perkara di atas.

Panduan ini adalah terpakai kepada semua pengguna di JTM termasuk kakitangan, pelajar, pembekal, pakarunding dan orang awam yang mencapai, mengurus, menyelenggara, memproses, memuat-turun, menyedia, memuat-naik, berkongsi, menyimpan dan menggunakan aset ICT JTM.

PRINSIP-PRINSIP

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

a. **Akses atas Panduan perlu mengetahui**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas Panduan "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 khas adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari masa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

c. **Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT JTM yang merangkumi:-

a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.
b) Memeriksa maklumat dengan tepat dan lengkap dari masa ke semasa.
c) Menyedia maklumat untuk digunakan oleh pengguna yang dibenarkan.

d. **Pengasingan**

Tugas-tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data yang dimasukkan ke dalam media elektronik hendaklah diasingkan kepada beberapa peringkat pengguna (*access level*). Ini bertujuan untuk mengelakkan akses yang tidak dibenarkan dan melindungi sumber ICT daripada dimonopoli dan dimanipulasi oleh seorang pengguna tertentu, sekaligus mengurangkan kesilapan dan seterusnya, mengekalkan kerahsiaan, integriti dan kebolehsediaan. Pada tahap minima, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:-

a) Persekitaran pembangunan untuk tujuan pembanguanan sistem dan ujian (*development and test environment*).
b) Persekitaran penerimaan sebagai persediaan sebelum memasuki persekitaran sebenar.
c) Persekitaran sebenar untuk sistem yang dioperasikan.
d) Pengasingan rangkaian, pelayan, komputer dan sumber-sumber lain kepada beberapa domain logikal untuk memudahkan kawalan dan juga bagi meminimakan kelemahan, ancaman dan risiko keselamatan.

e. **Pengauditan**

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

f. **Pematuhan**

Panduan Keselamatan ICT JTM 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 kesediaan (*availability*) dan kebolehcapaian (*accessibility*). Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana (*disaster recovery plan*)/kesinambungan perkhidmatan (*service contigency*); dan

h. **Saling Bergantungan**

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

Perkara 01 Pembangunan dan Penyelenggaraan Panduan

Panduan Keselamatan ICT		
010101	**Pelaksanaan Panduan**	
	Pelaksanaan Panduan ini akan dijalankan oleh Ketua Pengarah JTM dibantu oleh jawatankuasa pengurusan ICT di peringkat JTM (JPICT) yang terdiri daripada Timbalan Ketua Pengarah (*Chief Information Officer*) dan ahli-ahli jawatankuasa yang dilantik (sila rujuk lampiran 1). Dari peringkat JTM ianya dipanjangkan ke peringkat semua institut di bawah JTM (ILJTM) melalui satu jawatankuasa pengurusan ICT peringkat institut yang diketuai oleh pengarah institut selaku pengerusi (sila rujuk lampiran 2).	Ketua Pengarah
010102	**Penyebaran Panduan**	
	Panduan ini perlu disebarkan kepada dan diketahui oleh (*aware*) semua pengguna JTM, ILJTM dan pihak ketiga yang juga termasuk penguna perkhidmatan-perkhidmatan *online* JTM dan ILJTM.	ICTSO
010103	**Penyelenggaraan Panduan**	
	Panduan Keselamatan ICT JTM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, prosedur, perundangan (undang-undang siber), kepentingan sosial, arahan-arahan MAMPU serta perubahan polisi ICT kerajaan. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Panduan Keselamatan ICT JTM: a. Kenal pasti perubahan melalui mekanisma-mekanisma tertentu dan senaraikan perubahan yang diperlukan; b. Kemukakan cadangan pindaan secara bertulis kepada CIO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pengurusan ICT JTM (JPICT); c. Perubahan yang telah dipersetujui oleh JPICT JTM kemudiannya dimaklumkan kepada semua pengguna; d. Panduan ini hendaklah dikaji semula sekurang-kurangnya sekali setahun oleh JPICT berdasarkan perkara (a.) di atas dan maklumbalas-maklumbalas jawatankuasa pengurusan ICT di peringkat institut. e. Dari semasa ke semasa pengauditan perlaksanaan panduan ini hendaklah dilakukan untuk proses pemantauan dan pematuhan. f. Dokumen Panduan ini hendaklah menggunakan format dokumentasi sistem teknologi maklumat yang standard.	ICTSO

010104	Pengecualian Panduan	
	Panduan Keselamatan ICT JTM adalah terpakai kepada semua pengguna kemudahan ICT JTM dan pihak ketiga kecuali entiti-entiti yang memerlukan dan mempunyai kenyataan penafian (*disclaimer*).	Ahli-ahli jawatankuasa JPICT (JTM dan ILJTM)

Perkara 02 Keselamatan Organisasi

Infrastruktur Keselamatan Organisasi		
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 (KP) adalah seperti berikut: a. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Panduan Keselamatan ICT JTM; b. memastikan semua pengguna mematuhi Panduan Keselamatan ICT JTM; c. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Panduan Keselamatan ICT JTM.	Ketua Pengarah
020102	**Ketua Pegawai Maklumat (CIO)**	
	Timbalan Ketua Pengarah (TKP) adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggung jawab 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)**	
	Ketua Penolong Pengarah (KPP) adalah merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. mengurus keseluruhan program-program keselamatan ICT JTM; b. menguatkuasakan Panduan Keselamatan ICT JTM; c. memberi penerangan dan pendedahan berkenaan Panduan Keselamatan ICT JTM kepada semua pengguna; d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Panduan Keselamatan ICT JTM;	ICTSO

	e. menjalankan pengurusan risiko; f. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan 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) dan memaklumkannya kepada CIO; i. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti 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 Panduan Keselamatan ICT JTM; dan k. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
020104	**Pentadbir Sistem ICT - WAN**	
	Pegawai dilantik di peringkat ibupejabat oleh Ketua Pengarah JTM dan pegawai tersebut terlibat dengan ICT secara langsung, memenuhi syarat dan berketerampilan dalam bidang tersebut. Peranan dan tanggungjawab pentadbir sistem ICT - WAN adalah seperti berikut: a. mentadbir sistem ICT - WAN yang melibatkan penggunaan semua institut dan organisasi di bawah JTM; b. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan di bawah JPICT yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; c. menentukan tahap capaian dipatuhi berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Panduan Keselamatan ICT JTM; d. memantau aktiviti capaian harian pengguna dan menyediakan arkib aktiviti capaian ke media storan secara berkala; e. mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatal atau memberhentikannya dengan serta merta; f. menyimpan dan menganalisis rekod jejak audit; dan g. menyediakan laporan mengenai aktiviti capaian kepada	Pentadbir Sistem ICT - WAN

	JPICT berkenaan secara berkala.	
020105	**Pentadbir Sistem ICT – Institut**	
	Pegawai dilantik di peringkat institut oleh Pengarah Institut dan pegawai tersebut terlibat dengan ICT secara langsung, memenuhi syarat dan berketerampilan dalam bidang tersebut. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: a. mentadbir sistem ICT di institut masing-masing seperti pelayan*, client,* kawalan capaian, rangkaian dan lain-lain berkaitan ICT; b. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; c. menentukan tahap capaian dipatuhi berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Panduan Keselamatan ICT JTM; d. memantau aktiviti capaian harian pengguna; e. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatal atau memberhentikannya dengan serta merta; f. menyimpan dan menganalisis rekod jejak audit; dan g. menyediakan laporan mengenai aktiviti capaian kepada JPICT institut berkenaan secara berkala.	Pentadbir Sistem ICT - Institut
020106	**Pentadbir Sistem Pengkalan Data (Pusat Data JTM)**	
	Pegawai dilantik oleh Ketua Pengarah JTM dan pegawai tersebut berketerampilan dalam bidang Pengkalan Data dan mempunyai peranan dan tanggungjawab seperti berikut: a. menyediakan penduaan kepada pengkalan data di institut seperti menyedia strategi *backup* untuk pengkalan data dan membuat migrasi data lama kepada arkib data; b. memastikan *system service* sentiasa berfungsi dan beroperasi secara optimum; c. menentukan tahap capaian dipatuhi berdasarkan keperluan pengkalan data sebagaimana yang telah ditetapkan di dalam Panduan Keselamatan ICT JTM; d. memantau aktiviti capaian harian pengguna; e. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatal atau memberhentikannya dengan serta merta;	

	f. menyimpan dan menganalisis rekod jejak audit; dan g. menyediakan laporan mengenai aktiviti capaian kepada JPICT institut berkenaan secara berkala.	
020107	**Pentadbir Sistem Pengkalan Data (Institut)**	
	Pegawai dilantik di peringkat institut oleh Pengarah Institut dan pegawai tersebut berketerampilan dalam bidang Pengkalan Data dan mempunyai peranan dan tanggungjawab seperti berikut: h. menyediakan penduaan kepada pengkalan data di institut seperti menyedia strategi *backup* untuk pengkalan data dan membuat migrasi data lama kepada arkib data; i. memastikan *system service* sentiasa berfungsi dan beroperasi secara optimum; j. menentukan tahap capaian dipatuhi berdasarkan keperluan pengkalan data sebagaimana yang telah ditetapkan di dalam Panduan Keselamatan ICT JTM; k. memantau aktiviti capaian harian pengguna; l. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatal atau memberhentikannya dengan serta merta; m. menyimpan dan menganalisis rekod jejak audit; dan n. menyediakan laporan mengenai aktiviti capaian kepada JPICT institut berkenaan secara berkala.	
020108	**Pentadbir Sistem Web & E-mel (Ibu Pejabat JTM)**	
	Pegawai dilantik oleh Ketua Pengarah JTM dan pegawai tersebut berketerampilan dalam bidang Web dan Email. Peranan dan tanggungjawab seperti berikut: a. mentadbir laman web di ibu pejabat seperti memastikan maklumat web dikemaskini, *web service* berfungsi secara optimum, menyediakan ciri-ciri keselamatan pada web b. menyediakan akaun pengguna e-mel; c. mengambil tindakan yang bersesuaian dengan segera terhadap status akaun pengguna yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; d. menyimpan dan menganalisis rekod jejak audit web; dan e. menyediakan laporan mengenai aktiviti capaian web kepada JPICT berkenaan secara berkala.	
020109	**Pentadbir Sistem Web & E-mel (Institut)**	
	Pegawai dilantik di peringkat institut oleh Pengarah Institut dan pegawai tersebut berketerampilan dalam bidang Web dan	

	Email. Peranan dan tanggungjawab seperti berikut: a. mentadbir laman web di institut seperti memastikan maklumat web dikemaskini, *web service* berfungsi secara optimum, menyediakan ciri-ciri keselamatan pada web; b. mentadbir sistem e-mel dengan menyediakan akaun pengguna, perancangan kapasiti saiz storan e-mel dan lain-lain berkaitan dengan e-mel c. mengambil tindakan yang bersesuaian dengan segera terhadap status akaun pengguna yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; d. memastikan keselamatan sistem e-mel daripada semua ancaman seperti *spamming,* virus, *phishing, spying* dan lain-lain ancaman; e. memantau aktiviti capaian harian pengguna; f. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatal atau memberhentikannya dengan serta merta; g. menyimpan dan menganalisis rekod jejak audit e-mel dan web; dan h. menyediakan laporan mengenai aktiviti capaian e-mel dan web kepada JPICT institut berkenaan secara berkala.	
0201010	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti berikut: a. membaca, memahami dan mematuhi Panduan Keselamatan ICT JTM; b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. melaksanakan prinsip-prinsip Panduan Keselamatan ICT dan menjaga kerahsiaan maklumat JTM; d. melaksanakan langkah-langkah perlindungan seperti berikut :- 1. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; 2. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; 3. menentukan maklumat sedia untuk digunakan; 4. menjaga kerahsiaan kata laluan; 5. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; 6. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan,	Pengguna

	pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan 7. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. e. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; f. menghadiri program-program kesedaran mengenai keselamatan ICT; dan g. membaca dan memahami penyataan penafian *(disclaimer)* dan terma-terma perkhidmatan *(term of services).*	
Pihak Ketiga		
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.		
020201	**Keperluan Keselamatan Kontrak dengan Pihak Ketiga**	
	Akses kepada aset ICT JTM perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan. a. Panduan Keselamatan ICT JTM; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; d. Hak Harta Intelek; 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.	CIO, ICTSO, Semua Pentadbir Sistem dan Pihak Ketiga

Perkara 03 Kawalan dan Pengkelasan Aset

Akauntabiliti Aset Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JTM.		
030101	**Inventori Aset**	
	Semua aset ICT JTM hendaklah direkodkan. Ini termasuklah mengenalpasti aset, mengkelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya.	Pentadbir Sistem ICT
	Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah kawalannya.	Semua
Pengkelasan dan Pengendalian Maklumat Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
030201	**Pengkelasan 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; d. menjaga kerahsiaan kata laluan; e. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

Perkara 04 Keselamatan Sumber Manusia

Keselamatan ICT Dalam Tugas Harian Objektif: Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT JTM.		
040101	**Peranan dan Tanggungjawab Keselamatan**	
	Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah direkod dengan lengkap dan jelas samada di dalam fail meja, kontrak atau sebarang dokumen yang berkaitan, serta ianya perlu dipatuhi dan dilaksanakan seperti yang dinyatakan di dalam dokumen tersebut. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	Pengguna
040102	**Terma dan Syarat Pengguna**	
	Pengguna perlu memahami dan mematuhi terma dan syarat keselamatan ICT yang ditetapkan serta mematuhi peraturan semasa yang berkuat kuasa. Tatacara penggunaan kemudahan ICT pengguna adalah tertakluk kepada terma dan syarat keselamatan ICT yang ditetapkan sebagai garis panduan.	Pengguna
040103	**Perakuan Akta Rahsia Rasmi**	
	Mana-mana pengguna yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Pengguna
Menangani Insiden Keselamatan ICT Objektif: Meminimumkan kesan insiden keselamatan ICT.		
040201	**Pelaporan Insiden**	
	Insiden keselamatan ICT seperti berikut perlu dilaporkan kepada ICTSO atau JPICT ILJTM 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; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerapkali gagal dan komunikasi tersalah hantar; e. Berlaku percubaan menceroboh, penyelewengan dan	Pengguna

	insiden-insiden yang tidak diingini. Maklumat lanjut mengenai tatacara pelaporan insiden bolehlah merujuk kepada Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT)".	
Pendidikan		
Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.		
040301	**Program Kesedaran Keselamatan ICT**	
	Pengguna perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden perlu dilaksanakan dan diikuti oleh semua pengguna sebagai langkah proaktif yang boleh meminimumkan tahap ancaman keselamatan ICT JTM.	ICTSO dan JPICT ILJTM
Tindakan Tatatertib		
Objektif: Meningkat kesedaran dan pematuhan ke atas Panduan Keselamatan ICT JTM.		
040401	**Pelanggaran Panduan**	
	Sebarang pelanggaran Panduan Keselamatan ICT JTM boleh dikenakan tindakan tatatertib.	Pengguna

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 perlu di kenalpasti 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 keselamatan atau kamera; e. Menghadkan jalan keluar masuk; f. Mengadakan kaunter kawalan; g. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan h. Mewujudkan perkhidmatan pengawalan keselamatan.	KP, CIO, ICTSO, Pegawai Keselamatan ILJTM.
050102	**Kawalan Masuk Fizikal**	
	a. Setiap pengguna JTM 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. Setiap pelawat hendaklah mendaftar di pintu utama banguanan/kawasan JTM; e. Kehilangan pas mestilah dilaporkan dengan segera; f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT JTM;	Semua dan pelawat
050103	**Kawasan Larangan**	
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu	Semua

	sahaja, ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di JTM adalah bilik Ketua Pengarah, bilik-bilik Timbalan Ketua Pengarah, Pengarah, Timbalan Pengarah, bilik-bilik pelayan dan pusat data. Akses kepada bilik-bilik serta peralatan tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja dimana: a. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan b. Semua penggunaan peralatan yang melibatkan penghantaran, pengemaskinian dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	
Keselamatan Peralatan		
Objektif : Melindung 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 ciri-ciri keselamatan; c. Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan d. Sebarang bentuk penyelewengan atau salahguna 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; dan c. menggunakan perisian penyulitan (*encryption)* ke atas dokumen terperingkat yang disedia dan dihantar secara elektronik.	Semua

050203	**Media Storan**	
	Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat : a. Menyediakan 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. Media storan sebagai *backup* hendaklah direkodkan pergerakannya di dalam buku log.	Semua
050204	**Kabel Dan Peralatan Rangkaian**	
	Kabel komputer hendaklah dilindung 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. Kabel hendaklah dilindungi daripada kerosakan yang disengajakan atau tidak disengajakan; c. Laluan pemasangan kabel hendaklah dilindungi sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; d. Telefon, rangkaian kabel dan kabinet data hanyalah boleh diakses oleh individu yang dibenarkan sahaja; e. Kemudahan akses seperti *modem, access point* dan *router* perlu mempunyai mekanisme keselamatan; dan f. Semua peralatan seperti *backbone*, *router, switch* dan pelayan hendaklah disimpan di kawasan atau ruangan yang selamat.	ICTSO
050205	**Penyelenggaraan**	
	Perkakasan hendaklah diselengarakan 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;	Semua

	c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; d. Semua peralatan hendaklah mempunyai rekod selenggara yang teratur; dan e. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pegawai yang berkenaan.	
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 mengikut tatacara pengurusan aset alih kerajaan.	Semua
050207	**Peralatan di Luar Premis**	
	Bagi perkakasan yang dibawa keluar dari premis JTM, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan JTM: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c. Semua peralatan di luar premis hendaklah direkod dan mendapat kebenaran daripada Pegawai berkenaan.	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 JTM: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, disguising* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan c. Maklumat lanjut pelupusan bolehlah merujuk kepada Pekeliling Perbendaharaan semasa.	Semua

050209	***Clear Desk* dan *Clear Screen***	
	Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna 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; dan c. Dokumen yang mengandungi bahan-bahan sensitif hendaklah diambil segera dari pencetak.	Semua
	Keselamatan Persekitaran	
Objektif: Melindungi aset ICT JTM 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 sama ada untuk memperoleh, menyewa, mengubahsuai atau membeli hendaklah dirujuk terlebih dahulu kepada MAMPU. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil : 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 perkomputeran hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan perkomputeran; 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 diperiksa dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	Semua

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 (*Uniterruptible Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kiritikal seperti di bilik pelayan supaya mendapat bekalan kuasa yang sewajarnya; dan c. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.	ICTSO
050303	**Prosedur Kecemasan**	
	a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Manual Keselamatan JTM; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan yang dilantik.	Semua

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, dikenal pasti dan masih diguna pakai hendaklah didokumentasikan, disimpan dan dikawal mengikut tatacara pengurusan rekod yang dikeluarkan oleh Arkib Negara; b. Setiap prosedur mestilah mengandungi arahan-arahan yang lengkap, teratur dan jelas seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	ICTSO
060102	**Kawalan Perubahan**	
	a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai berkenaan; 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 atau pun tidak.	ICTSO
060103 Pengurusan Risiko / Ancaman ICT		
	Definisi a. Pengurusan risiko merangkumi proses mengenalpasti, menilai dan merangka langkah pencegahan risiko ancaman ICT. b. Pegawai-pegawai yang terlibat dalam proses pengurusan risiko mestilah mempunyai latar belakang dan disiplin berikut: • Pengurusan operasi pemprosesan data. • Pengaturcaraan sistem (Pengoperasian Sistem).	

	• Analisa sistem.
	• Program aplikasi.
	• Pengurusan pengkalan data.
	• Audit.
	• Keselamatan fizikal.
	• Komunikasi Rangkaian.
	• Isu perundangan.
	• Pengguna sistem
	
	Mengenalpasti Risiko
	
	Proses mengenalpasti ancaman dan risiko mengambil kira:
	
	• Faktor alam
	• Faktor manusia
	• Senarai maklumat dan aplikasi dalam system ICT JTM.
	• Meletakan senarai kepentingan dan tahap kritital.
	• Kenalpasti urusan atau gabungan urusan yang menggangu urusan operasi.
	• Kenalpasti elemen utama yang berisiko, sesetengah risiko adalah dikategori sebagai bukan keutamaan dan setengahnya adalah keutamaan tertinggi.
	• Penilaian terhadap Risiko dan Ancaman.
	
	Mengenalpasti Kesan Risiko
	
	Setelah mengenalpasti risiko dan ancaman secara menyeluruh, proses seterusnya adalah membuat penilaiannya terhadap kesan risiko. Elemen-elemen berikut mesti dinilai:
	
	• Kesan terhadap keselamatan
	  o JTM
	  o KSM
	  o Kerajaan
	  o Negara
	• Kesan Kos
	  o Kerugian
	  o Pembaikan
	• Kesan Sumber
	  o Sumber manusia
	  o Aset
	  o Maklumat
	• Masa baik pulih
	• Pelanggan
	• Imej jabatan
	
	Mengenalpasti Langkah Pencegahan
	
	Faktor-faktor yang dinilai dalam proses mengenalpasti langkah pencegahan adalah:
	
	• Kesahihan, tatacara dan polisi organisasi.
	• Keperluan pengguna dan had capaian.
	• Keperluan keupayaan Sistem ICT.
	• Keperluan jarak masa, ketepatan dan kesempurnaan.
	• Kos jangkahayat pengukuran keselamatan ICT
		ICTSO, JPICT

	jabatan. • Keteguhan relatif langkah keselamatan yang dicadangkan. • Kepercayaan terhadap lain-lain langkah keselamatan dalam pertimbangan. • Keperluan teknikal. • Desakan/pertimbangan budaya.	
Perancangan dan Penerimaan Sistem		
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
060201	**Perancangan Kapasiti**	
	a. Kapasiti sesuatu perkakasan seperti penambahan cakera keras, pelayan dan lebar jalur capaian 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 mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	JPICT
060202	**Penerimaan Sistem**	
	Semua sistem baru termasuklah sistem yang dikemas kini atau diubahsuai hendaklah memenuhi spesifikasi yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT
Perisian		
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya.		
060301	**Perlindungan dari Perisian Berbahaya**	
	a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus menggunakan *Intrusion Detection System* (IDS) dan mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian tulen; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini *pattern* anti virus dari semasa ke semasa; 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	Pentadbir Sistem LAN/WAN, Pengguna

	perisian. Klausa ini akan digunakan sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Mengedar amaran mengenai ancaman seperti serangan virus terhadap keselamatan aset ICT JTM.	
Housekeeping		
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh dicapai pada bila-bila masa.		
060401	**Penduaan**	
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Salinan *backup* hendaklah direkodkan dan di simpan di lokasi bangunan yang berlainan. a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan *backup* ke atas semua data mengikut kesesuaian operasi; c. Menguji sistem *backup* 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 merekod 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; c. Sekiranya wujud aktiviti-aktiviti tidak sah seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO; dan d. Mengarkib log ke media storan.	Pentadbir Sistem ICT, ICTSO
Pengurusan Rangkaian		
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
060501	**Kawalan Infrastruktur Rangkaian**	
	Infrastruktur Rangkaian mestilah di kawal 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;	Pentadbir Sistem ICT dan ICTSO

	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 *Final Acceptance Test (FAT)* 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 yang dibenarkan sahaja; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JTM; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer peribadi kecuali mendapat kebenaran Pentadbir Sistem ICT; h. Memasang perisian IDS bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JTM; i. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti kemasukan dari atau capaian pada laman web/Internet yang mengandungi maklumat atau unsur-unsur tidak sihat dan berbahaya yang boleh menjejaskan integriti kakitangan, sistem dan maklumat; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan JTM hendaklah mendapat kebenaran JPICT; k. Semua pengguna hanya dibenarkan menggunakan rangkaian JTM sahaja; dan l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optima.	
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 pegawai berkenaan terlebih dahulu.	Semua
060602	**Penghapusan**	
	Media yang mengandungi maklumat rahsia rasmi hedaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat. Pelupusan aset ICT hendaklah mengikut tatacara pengurusan	Semua

	aset alih kerajaan.	
060603	**Prosedur Pengendalian Maklumat**	
	a. Semua media hendaklah dilabelkan mengikut tahap sensiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian kepada pengguna yang sah sahaja; c. Menghadkan pengedaran data untuk tujuan yang dibenarkan; d. Penyelenggaraan media hendaklah dikawal dan direkodkan bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan e. Semua media hendaklah disimpan di tempat yang selamat.	Semua
060604	**Keselamatan Sistem Dokumentasi**	
	a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyediakan dan memantapkan lagi keselamatan sistem dokumentasi dalam rangkaian; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Pentadbir Sistem ICT, ICTSO
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 diperolehi 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 cipta terpelihara; e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh JTM; f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimana pun, kandungan perbincangan awam ini	Semua

	hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada Panduan dan peraturan yang telah ditetapkan; dan g. Pemasangan *proxy* atau aplikasi yang sesuai bagi membolehkan setiap laman web yang dilayari boleh di jejaki dan di rekodkan.	
060702	**Mel Elektronik**	
	a. Akaun atau alamat e-mel yang diperuntukkan oleh JTM 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 MAMPU; 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 (*attachment file*), sekiranya perlu semasa penghantaran; f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; dan j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat.	Pentadbir Sistem Web/Mel, pengguna

Perkara 07 Kawalan Capaian

Panduan Kawalan Capaian		
Objektif : Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT JTM.		
070101	**Keperluan Panduan**	
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkod, dikemas kini dan menyokong Panduan kawalan capaian pengguna sedia ada.	CIO,ICTSO
Pengurusan Capaian Pengguna		
Objektif : Mengawal capaian pengguna ke atas Prasarana dan Aplikasi ICT JTM.		
070201	**Akaun Pengguna**	
	Pentadbir sistem ICT yang berkenaan perlu menyediakan akaun pengguna pada setiap Aplikasi dan Prasarana ICT yang diwujudkan mengikut tahap capaian yang ditetapkan CIO pada aplikasi berkenaan merangkumi: a. Sistem Operasi Komputer dan Domain; b. *Web Proxy*; c. E-mel; d. TMS; e. Aplikasi lain sediada dan yang dibangunkan; f. Capaian Prasarana Rangkaian;dan g. Capaian Sistem Operasi Pelayan. Pengguna adalah 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/institut sahaja boleh digunakan; b. akaun pengguna mestilah unik dan katalaluan perlu kompleks dan perlu ditukar sekurang-kurangnya **enam** bulan sekali; c. akaun pentadbir perlu ditukar sekurang-kurangnya **tiga** bulan sekali; d. akaun pengguna yang diwujud pertama kali akan diberi tahap capaian paling minimum merujuk kepada aplikasi ICT berkenaan dan bersesuaian dengan tanggungjawab pengguna. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada ICTSO terlebih dahulu;	Semua

	e. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; f. penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan g. pentadbir sistem ICT boleh meminda capaian, membeku dan menamatkan akaun pengguna atas sebab-sebab berikut; i) pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan	
070202	**Jejak Audit / Log**	
	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 (fail log) dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubah suaian yang tidak dibenarkan.	Pentadbir Sistem ICT
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 ILJTM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Pentadbir sistem ICT perlu memastikan penggunaan akaun pengguna dan capaian ke sistem dilogkan. Aplikasi utama seperti dinyatakan dibawah perlu memenuhi keperluan minimum yang ditetapkan seperti berikut:	Pentadbir Sistem ICT, CIO

	Internet ILJTM menggalakkan penggunaan internet, termasuk perkhidmatan web dan e-mel, namun begitu penggunaan *Web Proxy Authentication* mesti dipraktikkan dan capaian pengguna mesti di log. Laporan capaian pengguna juga boleh dikeluarkan dan log pengguna perlu disimpan sekurang-kurangnya lima(5) tahun. **E-mel dan Aplikasi ICT** Sistem e-mel yang disediakan perlu memenuhi kehendak minimum berikut : a. Login pengguna perlu melalui saluran yang selamat bagi mengelak kecurian identiti;dan b. *Quota* akaun e-mel pengguna dipraktikkan (E-mel sahaja). Perkhidmatan E-mel dan Internet termasuk Aplikasi ICT perlu mematuhi **Garis Panduan Penggunaan Internet Dan E-mel Di Kementerian Sumber Manusia Serta Jabatan Di Bawahnya**. **Data dan Fail** Pengguna perlu memeriksa kesahihan data/fail dengan melakukan imbasan terhadap virus, *worm* atau *trojan* dan menyimpan di tempat yang disediakan. Pengguna dilarang mencapai, memindah dan menyalin data yang bukan dibawah kawalannya. Bagi memastikan kawalan capaian sistem dan aplikasi oleh pengguna 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-aktiviti yang tidak diingini; c. memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. memastikan penggunaan *session time out* untuk jangkamasa setengah jam setelah aplikasi ICT dibiarkan melahu (*idle*); e. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.	
Capaian Ke Prasarana ICT		
Objektif : Memastikan keselamatan maklumat apabila menggunakan kemudahan atau Prasarana ICT.		
070401	**Capaian Ke Prasarana ICT**	

	a. Hanya pengguna yang mempunyai akaun yang dibenarkan oleh ICTSO boleh menggunakan aplikasi dan prasarana ICT di JTM; b. Merekodkan aktiviti keluar masuk bilik pelayan bagi mengesan kehilangan atau pun kerosakan; c. Capaian aplikasi dan prasarana ICT perlu dilog dalam aplikasi secara automatik aplikasi yang digunakan. d. Prasarana ICT mudah alih hendaklah disimpan dan dikunci di tempat yang selamat; e. Hanya pengguna yang dibenarkan ICTSO boleh mencapai dan menggunakan *node* rangkaian di JTM;dan f. Capaian sistem dan aplikasi melalui jarak jauh atau *wireless* adalah digalakkan. Walau bagaimana pun, pentadbir sistem ICT perlu menggunakan ciri-ciri keselamatan (WEP/WPA/WPA2) dan hanya pengguna yang dibenarkan ICTSO sahaja dapat mencapai rangkaian.	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 mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji dan diperakui terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; d. Semua akses ke dalam sistem hendaklah menggunakan *secure socket layer (SSL)* bagi memastikan semua akaun dan kata laluan adalah selamat daripada pencerobohan.	Semua Pentadbir Sistem, ICTSO
Kriptografi		
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
080201	**Penyulitan *(Encryption)***	
	Setiap pengguna hendaklah membuat penyulitan ke atas semua sistem yang melibatkan maklumat sensitif atau kritikal bagi mengelakkan dari pendedahan dan penyelewengan maklumat berlaku. Penyulitan perlu untuk memastikan maklumat sensitif benar-benar selamat.	Semua
080202	**Tandatangan Digital**	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik seperti penggunaan tandatangan digital beserta kad pintar.	Semua
080203	**Pengurusan Kunci (*Public Key Infrastructure)***	
	Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

Sistem Fail		
Objektif: Memastikan supaya sistem fail dan aktiviti berkaitan beroperasi dengan baik dan selamat.		
080301	**Kawalan Sistem Fail**	
	a. Menyediakan kawalan keselamatan yang kukuh semasa melaksanakan perisian atau sistem aplikasi bagi mengurangkan risiko kerosakan kepada sistem pengoperasian; b. Proses pengemas kini sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; c. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksana atau digunakan selepas diuji dan diperakui; d. Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian program komputer; e. Mengaktifkan audit log bagi merekod semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; f. Melaksanakan salinan atau penduaan bagi meminimumkan risiko kerosakan dan kehilangan sistem fail.	Semua Pentadbir Sistem
Pembangunan dan Proses Sokongan		
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
080401	**Kawalan Perubahan**	
	a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum digunapakai. Perubahan versi hendaklah bebas dari ralat dan stabil.	Semua Pentadbir Sistem ICT

Perkara 09 Pengurusan Kesinambungan Perkhidmatan

Panduan 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 terutama dalam situasi kecemasan seperti serangan virus, bencana alam, *extended downtime* dan lain-lain lagi . Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Bagi memastikan keberkesanan pelan ini, ianya perlulah fleksibel untuk digunakan/diaplikasikan dalam sebanyak mungkin situasi kecemasan. Pelan ini mestilah memberi perhatian kepada perkara-perkara berikut :- a. mengenalpasti 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 kecemasan; dan e. menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.	CIO, ICTSO dan semua Pentadbir Sistem.
090102	**Pelan Kontigensi**	
	Pelan kontigensi yang mesti diwujudkan dan akan menjadi sebahagian daripada pelan kesinambungan perkhidmatan adalah :- a. Kontingensi Infrastruktur ICT *(ICT Infrastructure Contingency)*; b. Prosedur/ Proses *Backup* Aplikasi *(Application Backup Practices)*; c. Kontingensi Aplikasi Spesifik *(Specific Application Contingency)*; d. Kontingensi Rangkaian *(Network Contingency)*; e. Kontingensi PC & Sistem Kecil *(PC & Small System Contigency)*; f. Kontingensi Bekalan Kuasa *(Power Supply Contingency)*; dan g. Kontingensi Pengudaraan *(Air-conditioning Contingency).*	CIO, ICTSO dan semua Pentadbir Sistem

Berikut merupakan langkah-langkah yang perlu diambil bagi merangka pelan kesinambungan perkhidmatan yang berkesan dan menyeluruh :-

a. Penilaian Tahap Kritikal Aplikasi dan Data

i. Definasi Maklumat Awal Sistem *(Preliminary System Information)* dilakukan dengan mencatitkan nama organisasi dan sistem-sistem yang ada. Berikan deskripsi dan *architecture* bagi setiap sistem termasuklah tujuan sistem tersebut dan sebarang gambarajah sokongan atau yang berkaitan.

ii. Kenalpasti *Points of Contact* Sistem *(System Points of Contact)* iaitu hubungan *internal* dan *external* bagi setiap sistem untuk tujuan pengelasan hubungan sistem tersebut dengan seluruh sistem ICT organisasi. Segala fungsi sistem tersebut termasuklah fungsi tidak lansung perlulah diambil kira dalam mengenalpasti *points of contact* sesebuah sistem.

iii. Kenalpasti Sumber Sistem *(System Resources)* bagi semua aplikasi, data dan sumber ICT lain yang kritikal bagi kesinambungan perkhidmatan.

iv. Kenalpasti Peranan Kritikal *(Critical Roles)* dengan menyenaraikan individu yang mempunyai peranan kritikal dalam memastikan kesinambungan dan pemulihan perkhidmatan.

v. Tentukan Keutamaan Pemulihan *(Recovery Priorities)* berdasarkan tahap kritikal kebergantungan.

(Rujuk carta aktiviti pada lampiran 1)

b. Pelan *Backup* Data

Prosedur ini diperlukan bagi memastikan integriti, keselamatan dan ketersediaan data.

i. Kenalpasti Data Kritikal yang perlu di-*backup.*

ii. Tetapkan kadar kekerapan *backup* untuk *full* dan *incremental backup* bagi setiap aplikasi, system operasi dan data.

iii. Tetapkan tempoh penyimpanan *backup* dengan menentukan *retention period* bagi setiap *backup* aplikasi, sistem operasi dan data dengan mengambil kira kekerapan *full* dan *incremental backup*.

iv. Kenalpasti tempat media penyimpanan *(storage media) dengan* memastikan tempat penyimpanan sistem yang asal dan sistem yang di-*backup* tidak disimpan atau terletak di tempat yang sama.

v. Tentukan proses pengambilan *backup (retrieval)* dengan menentukan personel yang bertanggungjawab dan diberi kebenaran untuk memasuki tempat penyimpanan storan *backup*.

(Rujuk carta aktiviti pada lampiran 2)

c. Pelan Pemulihan

i. Tetapkan proses pemberitahuan *(notification process)* kepada pihak berkaitan termasuk pasukan pelaksana pelan kontingensi apabila berlakunya senario yang didefinisikan sebagai kecemasan.

ii. Kenalpasti pasukan pelaksana yang bertanggungjawab melaksanakan pelan pemulihan.

iii. Tentukan prosedur penilaian kerosakan dengan mengenalpasti dan menyenaraikan prosedur yang boleh digunakan dalam proses menilai kerosakan.

iv. Tentukan prosedur pemulihan aplikasi dan data berdasarkan keutamaan pemulihan, tentukan urutan prosedur pemulihan aplikasi dan data.

(Rujuk carta aktiviti pada lampiran 3)

d. Ujicuba dan Pindaan Pelan Kontingensi

i. Kenalpasti elemen pelan kontingensi untuk diujicuba dengan menyenaraikan elemen yang dikenalpasti untuk diujicuba dan dipinda secara berkala bagi memastikan pelan kontingensi adalah tepat, efektif dan memenuhi keperluan terkini.

ii. Tetapkan objektif ujicuba bagi setiap elemen dan objektif menyeluruh ujicuba.

iii. Kenalpasti peranan individu yang terlibat dalam aktiviti ujicuba dengan menyenaraikan individu yang terlibat beserta peranan spesifik yang akan dimainkan dalam proses ujicuba .

iv. Tetapkan senario ujicuba dengan menyenaraikan senario yang boleh digunakan dalam ujicuba. Perhatian perlu diberikan kepada senario yang mempunyai kebarangkalian yang tinggi untuk berlaku.

v. Laksanakan ujicuba dan dokumenkan keputusan direkodkan dan disemak bersama personel yang berkaitan.

vi. Pinda pelan kontingensi agar ianya selari dengan keperluan sistem, prosedur, struktur organisasi dan polisi terkini. Pindaan berkala perlu ditetapkan disamping dijalankan setiap kali terdapat perubahan yang memberi kesan kepada:

- Keperluan operasi *(operational requirements)*;
- Keperluan keselamatan *(security requirements)*;
- Prosedur teknikal *(technical procedures)*;
- Perubahan *hardware, software* atau peralatan lain; dan
- Perubahan pada pasukan pelaksana atau maklumat ahli pasukan yang boleh dihubungi.

090103	Penduaan	
	a. Membuat penduaan ke atas semua sistem-sistem ICT yang kritikal sebagai kontigensi bagi memastikan pemulihan dapat dilaksanakan; b. Penduaan hendaklah dibuat secara berkala bagi mengurangkan beban pembangunan semula serta mempercepatkan proses pemulihan sistem; c. Salinan-salinan penduaan mesti disimpan dengan selamat di tempat berlainan dari salinan asal dan dikawal; dan d. Prosedur pemulihan mestilah disemak dan diuji secara berjadual bagi memastikan prosedur berkenaan sentiasa boleh dipraktikkan.	Pentadbir Sistem ICT

Perkara 10 Pematuhan

Pematuhan dan Keperluan Perundangan		
Objektif : Menghindar dan mengesan sebarang pelanggaran Panduan Keselamatan ICT JTM.		
100101	**Pematuhan Panduan**	
	Setiap pengguna di JTM hendaklah membaca, memahami dan mematuhi Panduan Keselamatan ICT JTM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa.	Semua
100102	**Kaedah Pematuhan**	
	Pamatuhan ini dicapai melalui: a. Proses kajian untuk memantau dan menilai keberkesanaan mematuhi langkah-langkah keselamatan yang telah dikuatkuasakan. b. Merumuskan pelan pematuhan. c. Program keselamatan secara lazim untuk memastikan standard dan prosidur keselamatan dipatuhi. d. Menguatkuasakan amalan melapor sebarang peristiwa yang mengancam keselamatan dipatuhi dan seterusnya mengambil tindakan pembetulan.	CIO, ICTSO, Pentadbir Sistem ICT
100103	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JTM: a. Arahan Keselamatan; b. Pekeling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; c. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)"; d. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; e. Akta Tandangan Digital 1997; f. Akta Jenayah Komputer 1997; g. Akta Hakcipta (Pindaan) Tahun 1997;	Semua

	h. Akta Komunikasi dan Multimedia 1998; i. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); j. Dasar Keselamatan JTM; k. Garis Panduan Penggunaan Internet Dan E-Mel Di Kementerian Sumber Manusia Serta Jabatan Di Bawahnya; dan l. Information Security Management Standards (MS ISO 17799) oleh Jabatan Standard Malaysia dan SIRIM.	