DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

MAJLIS BANDARAYA PULAU PINANG

18 SEPTEMBER 2018

VERSI 1.1

DASAR KESELAMATAN ICT MBPP

DASAR KESELAMATAN ICT MBPP

DASAR KESELAMATAN ICT MBPP

DASAR KESELAMATAN ICT MBPP

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUAT KUASA
09 Disember 2012	1.0	Setiausaha Perbandaran	10 Disember 2013
15 September 2018	1.1	Setiausaha Bandaraya	25 September 2018

REKOD PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN
15 Sept 2018	1.2	Pindaan: 1) Nama Agensi daripada Majlis Perbandaran Pulau Pinang kepada Majlis Bandaraya Pulau Pinang. 2) Nama jawatan daripada Yang DiPertua kepada Datuk Bandar dan daripada Setiausaha Perbandaran kepada Setiausaha Bandaraya.
15 Sept 2018	1.2	**020103 Pegawai Keselamatan ICT (ICTSO) :** Pertambahan peranan dan tanggungjawab iaitu : (l) Koordinator Pengurusan Kesinambungan Perkhidmatan (Koordinator PKP).

DASAR KESELAMATAN ICT MBPP

TUJUAN

Tujuan dasar ini adalah untuk menggariskan peraturan-peraturan yang perlu dipatuhi oleh semua warga MAJLIS BANDARAYA PULAU PINANG (MBPP) untuk menjaga keselamatan dan aset teknologi maklumat dan komunikasi (ICT). Dengan adanya peraturan ini adalah diharapkan semua pengguna di MBPP sedar tentang tanggungjawab dan peranan mereka dalam melindungi aset ICT MBPP. Oleh itu tahap keselamatan ICT dan langkah-langkah mengurangkan risiko ancaman dari dalam dan luar ke atas sistem dan infrastruktur ICT dapat dipertingkatkan.

OBJEKTIF

Objektif Dasar Keselamatan ICT adalah seperti berikut:

a. Memastikan pengawalan dan pengurusan keselamatan ke atas perkakasan, perisian, aplikasi dan operasi komputer.
b. Dasar Keselamatan ICT MBPP diwujudkan untuk menjamin kesinambungan urusan MBPP dengan meminimumkan kesan insiden keselamatan ICT.
c. Mengelakkan berlakunya percanggahan data dan maklumat di MBPP.
d. Memastikan aset ICT terlindung daripada ancaman pencerobohan/penggodaman, kecurian data, serangan virus dan penafian perkhidmatan.
e. Mencegah kes-kes penyalahgunaan serta kehilangan aset ICT MBPP.

SKOP

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti :

a. Perkakasan - Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan agensi. 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 agensi;
c. Perkhidmatan - Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh :

- Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain.
- Sistem halangan akses seperti sistem kad akses.
- 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 agensi. Contoh:

- Sistem dokumentasi, prosedur operasi, rekod-rekod agensi, 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 agensi bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

f. Dasar ini adalah terpakai oleh semua pengguna di MBPP termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT MBPP.

PRINSIP-PRINSIP

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

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 MBPP.

d. Pengasingan

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. 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 MBPP hendaklah dibaca, difahami dan dipatuhi bagi mengelak 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.

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

010101	**Perlaksanaan Dasar**	
		Tanggungjawab
	Pelaksanaan dasar ini akan dijalankan oleh Yg. Bhg. Datuk Bandar dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), Pegawai Keselamatan MBPP, Pengurus Teknikal dan Pentadbir Sistem dan semua Pegawai/Penolong Pegawai Teknologi Maklumat.	Datuk Bandar
010102	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua pengguna MBPP (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO
010103	**Penyebaran 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 mempunyai hubung kait dengan penyelenggaraan Dasar Keselamatan ICT MBPP : a. kenal pasti dan tentukan perubahan yang diperlukan; b. kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Kerja ICT (MJKICT) MBPP; c. perubahan yang telah dipersetujui oleh MJKICT dimaklumkan kepada semua pengguna; dan d. dasar ini hendaklah dikaji semula sekurang-kurangnya oleh ICTSO sekali setahun.	ICTSO

010104	Pengecualian Dasar	
	Dasar keselamatan ICT MBPP adalah terpakai kepada semua pengguna-pengguna ICT MBPP 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	**Datuk Bandar**	
		Tanggungjawab
	Peranan dan tanggungjawab Datuk Bandar adalah seperti berikut: a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MBPP. b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MBPP. c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi. d. Memastikan penilainan risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MBPP.	
020102	**Setiausaha Bandaraya**	
	Peranan dan tanggungjawab beliau adalah seperti berikut: a. Membantu Datuk Bandar dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT. b. Menentukan keperluan keselamatan ICT. c. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.	CIO
020103	**Pegawai Keselamatan ICT (ICTSO)**	
	Ketua Bahagian Teknologi Maklumat juga merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut : a. Mengurus keseluruhan program-program keselamatan ICT MBPP. b. Menguatkuasakan Dasar Keselamatan ICT MBPP.	ICTSO

	c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MBPP kepada semua pengguna. d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keperluan ICT MBPP. 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 pasti punca ancaman atau insiden keselamatan ICT dan memperlakukan langkah-langkah baik pulih dengan segera. j. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT MBPP. k. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
020104	**Pengurus Teknikal**	
	Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat yang dilantik oleh ICTSO adalah merupakan Pengurus Teknikal MBPP. Peranan dan tanggungjawab Pengurus Teknikal adalah seperti berikut:	

	a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MBPP. b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MBPP. c. Menentukan kawalan akses semua pengguna terhadap aset ICT MBPP. d. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO. e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MBPP.	
020105	**Pentadbir Sistem**	
	Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat yang dilantik oleh ICTSO adalah merupakan Pentadbir Sistem ICT MBPP. 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 MBPP. c. Memantau aktiviti capaian harian pengguna. d. Mengenalpasti 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. f. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	

020106	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MBPP. 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 MBPP. e. Melaksanakan langkah-langkah perlindungan seperti 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. 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. h. Menandatangani surat akuan pematuhan Dasar Keselamatan ICT MBPP.	

Pihak Ketiga		
Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga		
020201	**Keperluan Keselamatan Kontrak dengan Pihak Ketiga**	
	Akses kepada aset ICT MBPP perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan. a. Dasar Keselamatan ICT MBPP. b. Tapisan Keselamatan. c. Perakuan Akta Rahsia Rasmi 1972. d. Hak Harta Intelek. **Rujukan:** 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

Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MBPP.

030101 Inventori Aset

		Tanggungjawab
	Semua aset ICT MBPP hendaklah direkodkan. Ini termasuklah mengenai 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.	Pengurus Teknikal ICT/ Pegawai Aset Jabatan

Pengelasan Dan Pengendalian Maklumat

Objektif : Memastikan setiap maklumat atau aset ICT diberi tahap perlindungan yang bersesuaian.

030102 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 d. Terhad	Pegawai Pengkelasan Dokumen

030103	**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 penyimpanan, g. penghantaran, penyampaian, pertukaran dan pemusnahan. h. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

Perkara 04 : KESELAMATAN SUMBER MANUSIA

Keselamatan Sumber Manusia

Objektif : Meminimum risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT MBPP.

040101	**Tanggungjawab Keselamatan**	
		Tanggungjawab
	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 MBPP yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	Semua
040103	**Perakuan Akta Rasmi**	
	Warga MBPP yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua

Menangani Insiden Keselamatan

Objektif : Meminimum kesan insiden keselamatan ICT

040201	**Pelaporan Insiden**	
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera iaitu:	Semua

	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 kerap kali gagal dan komunikasi tersalah hantar. e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. **Rujukan:** Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT"	Semua
Pendidikan Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.		
040301 Program Kesedaran Keselamatan ICT		
	Setiap pengguna di MBPP 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 MBPP.	ICTSO
Tindakan Tatatertib Objektif : Meningkatkan kesedaran dan pematuhan ke atas Dasar Keselamatan ICT MBPP.		
040401 Pelanggaran Dasar		
	Pelanggaran Dasar Keselamatan ICT MBPP akan 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

		Tanggungjawab
	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 CCTV e. Menghadkan jalan keluar masuk. f. Mengadakan kaunter kawalan. g. Menyediakan tempat atau bilik khas untuk pelawat-pelawat. h. Mewujudkan perkhidmatan kawalan keselamatan.	CIO dan Pegawai Keselamatan

050102 Kawalan Masuk Fizikal

	a. Setiap pengguna MBPP 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.	Semua

	c. Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara. d. Kehilangan pas mestilah dilaporkan dengan segera. e. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT MBPP.	Semua
050103	**Kawasan Larangan**	
	a. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di MBPP adalah bilik Datuk Bandar, Setiausaha Bandaraya, bilik fail, bilik *handheld* dan bilik Pelayan ICT. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu. b. Pihak ketiga adalah dilarang sama sekali untuk memasuk 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. c. Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	Semua

Keselamatan Peralatan Objektif : Melindungi peralatan dan maklumat		
050201	**Perkakasan**	
		Tanggungjawab
	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. d. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada Pengurus Teknikal.	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. 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-langhkah 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. 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 : Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan. a. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan. b. Melindungi laluan pemasangan kabel sepenuhnya.	Semua
050205	**Penyelenggaraan**	
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti. a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan.	ICTSO dan Pengurus Teknikal

	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. d. Semua penyelenggaraan mestilah mendapat kebenaran daripada ICTSO.	ICTSO dan Pengurus Teknikal
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: Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan. a. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Semua
050207	**Peralatan Di Luar Premis**	
	Bagi perkakasan yang dibawa keluar dari premis MBPP, langkah-langkah keselamatan hendaklah diadakan dengan mengambilkira risiko yang wujud di luar kawasan MBPP: a. Peralatan perlu dilindungi dan dikawal sepanjang masa. b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-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 MBPP.	Semua dan Jawatankuasa Pelupusan

050209	***Clear Desk* Dan *Clear Screen***	
	Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakkan, 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 sav*er atau log keluar apabila meninggalkan komputer. b. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci.	Semua
050210	**Penggunaan *Thumb/Pen Drive***	
	Penggunaan *thumb/pen drive* adalah keperluan kepada pengguna untuk menyimpan data/maklumat secara sementara/kekal. Terdapat beberapa perkara yang perlu diberi perhatian mengenai penggunaan *thumb/pen drive* : a. Pemohon perlu mendapat kebenaran daripada Ketua Jabatan terlebih dahulu. b. Spesifikasi kerja perlu dinyatakan supaya penggunaan *thumb/pen drive* tidak disalahgunakan. c. Pemohon dan Ketua Jabatan bertanggungjawab sepenuhnya berkenaan penggunaan *thumb/pen drive* tersebut. d. Semua maklumat yang ada didalam *thumb/pen drive* yang berkaitan dengan segala maklumat Jabatan jika hilang adalah tanggungjawab sepenuhnya oleh pemohon. e. Penggantian bagi kehilangan *thumb/pen drive* akibat kecuaian TIDAK akan dilayan.	Semua

Keselamatan Persekitaran Objektif : Melindungi aset ICT MBPP dari sebarang bentuk ancaman persekitaran yang disebabkan oleh alam, kesilapan, kecuaian atau kemalangan.		
050301	**Kawalan Persekitaran**	
		Tanggungjawab
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Ketua Bahagian Teknologi Maklumat. 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. 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. b. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT. c. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer. d. 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.	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 (*Uninterruptable Power System*) dan penjana (generator) boleh digunakan bagi perkhidmatan kritikal seperti di bilik pelayan supaya mendapat bekalan kuasa berterusan. c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Semua

Perkara 06 : PENGURUSAN OPERASI DAN KOMUNIKASI

Pengurusan Prosedur Operasi

Objektif : Memastikan perkhidmatan dan pemprosesan maklumat dapat beroperasi dengan betul dan selamat.

060101	**Pengendalian Prosedur**	
		Tanggungjawab
	a. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti 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. 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 Ketua Bahagian Teknologi Maklumat. 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. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan	Semua

	c. 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. Mengenal pasti semua jenis insiden keselamatan ICT 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. d. Menyediakan tindakan pemulihan segera .	ICTSO/ Pengurus Teknikal
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. 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.	ICTSO/ Pentadbir Sistem

060202	**Penerimaan Sistem**	
	Semua system baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	ICTSO/ Pentadbir Sistem
Perisian Berbahaya Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti *virus* dan *trojan*.		
060301	**Perlindungan dan Perisian Berbahaya**	
	a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti *anti virus* dan *Intrusion Detection System* (IDS) dan mengikut prosedur penggunaan yang betul dan selamat. b. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya. c. Mengemas kini *pattern anti virus* setiap minggu. d. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat. e. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya. f. 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. g. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan. h. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	ICTSO/ Pengurus Teknikal

Housekeeping Objektif : Melindungi integriti 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 terbaru. b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi. c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan	Pentadbir Sistem
060402	**Sistem Log**	
	a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna. b. Mewujudkan satu sistem log secara berpusat dan perlu dibuat pendua. c. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera. d. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem dan Pengurus Teknikal

Pengurusan Rangkaian Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
060501	**Kawalan Infrastruktur 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 MBPP. g. Semua perisian *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO. h. Memasang perisian *Intrusion Detection System (IDS)* atau *Intrusion Preventive System (IPS)* bagi mengesan/menghalang sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem	ICTSO/ Pengurus Teknikal

	dan maklumat MBPP. i. Sebarang penyambungan rangkaian yang bukan dibawah kawalan MBPP hendaklah mendapat kebenaran ICTSO. j. Semua pengguna hanya dibenarkan menggunakan rangkaian MBPP sahaja k. Penggunaan modem atau teknologi lain seperti 3G Broadband perlu mendapatkan kebenaran ICTSO. l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	ICTSO/ Pengurus Teknikal
Pengurusan Media Objektif : Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak terkawal. Media bermaksud sebarang bahan termasuk pita, CD, DVD, filem, disket, *thumb drive*, laptop *hard disk*, surat, dokumen dan manual.		
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. 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 penyampaian dokumentasi mempunyai ciri-ciri keselamatan. b. Menyediakan dan memantapkan keselamatan sistem dokumentasi. c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Semua
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 terpelihara. e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MBPP. 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.	Semua

	Rujukan Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi Kerajaan"	
060702	**Mel Elektronik**	
	a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MBPP 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 MBPP. c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan. d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul. e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi lima belas (15) 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-mel. h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan.	Semua

	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. **Rujukan** Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi Kerajaan”	

Perkara 07 : KAWALAN CAPAIAN

Dasar Kawalan Capaian

Objektif : Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT MBPP.

070101 Keperluan Dasar

		Tanggungjawab
	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.	ICTSO/ Pentadbir Sistem

Pengurusan Capaian Pengguna

Objektif : Mengawal capaian pengguna ke atas aset ICT MBPP.

070102 Akaun pengguna

	Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi : a. Permohonan penggunaan sistem mestilah diisi melalui borang seperti yang dikuatkuasakan oleh Bahagian Teknologi Maklumat. b. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan. c. Akaun pengguna mestilah unik. d. Akaun pengguna yang diwujud 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. 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.	Semua

	g. 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. iii. Bertukar ke agensi lain. iv. Bersara. v. Ditamatkan perkhidmatan	Semua
070201	**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. 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 pengubah suaian yang tidak dibenarkan.	Pentadbir Sistem

Kawalan Capaian Sistem dan Aplikasi Objektif : Melindungi sistem maklumat dan aplikasi sedia ada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.		
070301	**Sistem Maklumat dan Aplikasi**	
		Tanggungjawab
	Capaian kepada proses dan maklumat di MBPP 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-aktiviti yang tidak diingini. c. Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan. d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah. e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	ICTSO/ Pentadbir Sistem

Peralatan Komputer Mudah Alih Objektif : Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.		
070401	**Penggunaan Peralatan Komputer Mudah Alih**	
		Tanggungjawab
	a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan. b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. c. Komputer mudah alih yang dibawa keluar daripada premis Majlis untuk urusan pejabat perlu mendapatkan kelulusan Ketua Jabatan terlebih dahulu. d. Kehilangan peralatan tersebut adalah tanggungjawab individu kerana insurans hanya meliputi kawasan pejabat dan urusan rasmi seperti bengkel, seminar dan aktiviti lain.	

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**	
		Tanggungjawab
	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. 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.	Pentadbir Sistem

Kriptografi

Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat.

080201	**Penyulitan**	
	Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia pada setiap masa.	Semua
080202	**Pengurusan Kunci**	
	Pengurusan kunci 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**	
		Tanggungjawab
	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 aturcara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji. c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem
Pembangunan dan Proses Sokongan Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
080401	**Kawalan Perubahan**	
	Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Pentadbir Sistem

DASAR KESELAMATAN ICT MBPP

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**	
		Tanggungjawab
	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 Jawatankuasa Pemandu PKP (Perkhidmatan Kesinambungan Perkhidmatan).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. b. Membuat penduaan. c. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	ICTSO/ Pengurus Teknikal/ Pentadbir Sistem

Perkara 10 : PEMATUHAN

Pematuhan dan Keperluan Perundangan

Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran Dasar Keselamatan ICT MBPP.

100101 Pematuhan Dasar

		Tanggungjawab
	Setiap pengguna di MBPP hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MBPP dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di MBPP 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.	

100102 Keperluan Perundangan

	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MBPP : a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; c. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS); d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; f. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;	

	g. Akta Tanda Tangan Digital 1997; dan h. Akta Genayah Komputer 1997; i. Akta Hak Cipta (Pindaan) Tahun 1997; dan j. Akta Komunikasi dan Multimedia 1998; k. Pekeliling-pekeliling dan Prosedur-prosedur yang dikeluarkan dari masa kesemasa.	

MAJLIS BANDARAYA PULAU PINANG

Disahkan Oleh

.....

IR.ADDNAN BIN MOHD RAZALI
SETIAUSAHA BANDARAYA

TARIKH DIKEMASKINI 28/09/2018

JABATAN KHIDMAT PENGURUSAN

BAHAGIAN TEKNOLOGI MAKLUMAT