

# DASAR KESELAMATAN ICT MBKT

ISI KANDUNGAN	MUKA SURAT
<b>PENGENALAN</b>	5
<b>OBJEKTIF</b>	5
<b>PENYATAAN DASAR</b>	5
<b>SKOP</b>	7
<b>PRINSIP-PRINSIP</b>	8
<b>BIDANG 1 – PEMBANGUNAN DAN PENYELENGGARAAN DASAR</b>	11
1.1 Dasar Keselamatan ICT	11
1.1.1 Pelaksanaan Dasar	11
1.1.2 Penyebaran Dasar	11
1.1.3 Penyelenggaraan Dasar	12
1.1.4 Pengecualian Dasar	12
<b>BIDANG 2 – ORGANISASI KESELAMATAN</b>	13
2.1 Infrastruktur Organisasi Dalam	13
2.1.1 Y.Bhg. Datuk Bandar Majlis Bandaraya Kuala Terengganu	13
2.1.2 Ketua Pegawai Maklumat (CIO)	14
2.1.3 Pengurus ICT	14
2.1.4 Pegawai Keselamatan ICT (ICTSO)	15
2.1.5 Pentadbir Sistem ICT	16
2.1.6 Pengguna	16
2.2 Pihak Ketiga	17
2.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	17
<b>BIDANG 3 – PENGURUSAN ASET</b>	19
3.1 Akauntabiliti Aset	19
3.1.1 Inventori Aset ICT	19
3.2 Pengelasan dan Pengendalian Maklumat	20
3.2.1 Pengelasan Maklumat	20
3.2.2 Pengendalian Maklumat	20
<b>BIDANG 4 – KESELAMATAN SUMBER MANUSIA</b>	23
4.1 Keselamatan Sumber Manusia Dalam Tugas Harian	23
4.1.1 Sebelum Perkhidmatan	23
4.1.2 Dalam Perkhidmatan	24
4.1.3 Bertukar Atau Tamat Perkhidmatan	25
<b>BIDANG 5 – KESELAMATAN FIZIKAL DAN PERSEKITARAN</b>	27
5.1 Keselamatan Kawasan	27
5.1.1 Kawalan Kawasan	27
5.1.2 Kawalan Masuk Fizikal	28
5.1.3 Kawasan Larangan	29
5.2 Keselamatan Peralatan	29
5.2.1 Peralatan ICT	29

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 1 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

---

5.2.2	Media Storan	31
5.2.3	Media Tandatangan Digital	32
5.2.4	Media Perisian dan Aplikasi	32
5.2.5	Penyelenggaraan Perkakasan	33
5.2.6	Peralatan di Luar Premis	33
5.2.7	Pelupusan Perkakasan	34
5.3	Keselamatan Persekitaran	35
5.3.1	Kawalan Persekitaran	35
5.3.2	Bekalan Kuasa	37
5.3.3	Kabel	37
5.3.4	Prosedur Kecemasan	38
5.4	Keselamatan Dokumen	38
5.4.1	Dokumen	38
<b>BIDANG 6 – PENGURUSAN OPERASI DAN KOMUNIKASI</b>		<b>39</b>
6.1	Pengurusan Prosedur Operasi	39
6.1.1	Pengendalian Prosedur	39
6.1.2	Kawalan Perubahan	39
6.1.3	Pengasingan Tugas dan Tanggungjawab	40
6.2	Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	41
6.2.1	Perkhidmatan Penyampaian	41
6.3	Perancangan dan Penerimaan Sistem	41
6.3.1	Perancangan Kapasiti	41
6.3.2	Penerimaan Sistem	42
6.4	Perisian Berbahaya	42
6.4.1	Perlindungan dari Perisian Berbahaya	42
6.4.2	Perlindungan dari Mobile Code	43
6.5	Housekeeping	43
6.5.1	Backup	44
6.6	Pengurusan Rangkaian	44
6.6.1	Kawalan Infrastruktur Rangkaian	45
6.7	Pengurusan Media	46
6.7.1	Penghantaran dan Pemindahan	46
6.7.2	Prosedur Pengendalian Media	46
6.7.3	Keselamatan Sistem Dokumentasi	47
6.8	Pengurusan Pertukaran Maklumat	47
6.8.1	Pertukaran Maklumat	48
6.8.2	Pengurusan Mel Elektronik (E-mel)	48
6.9	Perkhidmatan E-Dagang (Electronic Commerce Services)	50
6.9.1	E-Dagang	50
6.9.2	Maklumat Umum	51
6.10	Pemantauan	51
6.10.1	Pengauditan dan Forensik ICT	51
6.10.2	Jejak Audit	52

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 2 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

6.10.3	Sistem Log	53
6.10.4	Pemantauan Log	53
<b>BIDANG 7 – KAWALAN CAPAIAN</b>		<b>55</b>
7.1	Dasar Kawalan Capaian	55
7.1.1	Keperluan Kawalan Capaian	55
7.2	Pengurusan Capaian Pengguna	56
7.2.1	Akaun Pengguna	56
7.2.2	Hak Capaian	57
7.2.3	Pengurusan KataLaluan	57
7.2.4	Clear Desk dan Clear Screen	58
7.3	Kawalan Capaian Rangkaian	59
7.3.1	Capaian Rangkaian	59
7.3.2	Capaian Internet	60
7.4	Kawalan Capaian Sistem Pengoperasian	61
7.4.1	Capaian Sistem Pengoperasian	62
7.4.2	Kad Pintar	63
7.5	Kawalan Capaian Aplikasi dan Maklumat	63
7.5.1	Capaian Aplikasi Maklumat	63
7.6	Peralatan Mudah Alih dan Kerja Jarak Jauh	64
7.6.1	Peralatan Mudah Alih	64
7.6.2	Kerja Jarak Jauh	64
<b>BIDANG 8– PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM</b>		<b>65</b>
8.1	Keselamatan Dalam Membangunkan Sistem dan Aplikasi	65
8.1.1	Keperluan Keselamatan Sistem Maklumat	65
8.1.2	Pengesahan Data Input dan Output	66
8.2	Kawalan Kriptografi	66
8.2.1	Enkripsi	66
8.2.2	Tandatangan Digital	66
8.2.3	Pengurusan Infrastruktur Kunci Awam (PKI)	66
8.3	Keselamatan Fail Sistem	67
8.3.1	Kawalan Fail Sistem	67
8.4	Keselamatan Dalam Proses Pembangunan dan Sokongan	68
8.4.1	Prosedur Kawalan Perubahan	68
8.4.2	Pembangunan Perisian Secara Outsource	69
8.5	Kawalan Teknikal Keterdedahan (Vulnerability)	69
8.5.1	Kawalan dari Ancaman Teknikal	69
<b>BIDANG 9 – PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN</b>		<b>71</b>
9.1	Mekanisme Pelaporan Insiden Keselamatan ICT	71
9.1.1	Mekanisme Pelaporan	71
9.2	Pengurusan Maklumat Insiden Keselamatan ICT	72
9.2.1	Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	72
<b>BIDANG 10 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN</b>		<b>75</b>

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 3 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

---

10.1	Dasar Kesenambungan Perkhidmatan	75
10.1.1	Pelan Kesenambungan Perkhidmatan	75
<b>BIDANG 11 – PEMATUHAN</b>		79
11.1	Pematuhan dan Keperluan Perundangan	79
11.1.1	Pematuhan Dasar	79
11.1.2	Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	80
11.1.3	Pematuhan Keperluan Audit	80
11.1.4	Keperluan Perundangan	80
11.1.5	Pelanggaran Dasar	82

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 4 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

---

## PENGENALAN

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

## OBJEKTIF

DKICT Majlis Bandaraya Kuala Terengganu diwujudkan untuk menjamin kesinambungan urusan Majlis Bandaraya Kuala Terengganu dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala objektif utama keselamatan ICT Majlis Bandaraya Kuala Terengganu ialah seperti berikut :

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

## PENYATAAN DASAR

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

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 5 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

---

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

- (a) Melindungi maklumat rahsia rasmi dan maklumat rahsia kerajaan dari capaian tanpa kuasa yang sah;
- (b) Menjamin setiap maklumat adalah tepat dan sempurna;
- (c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
- (d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

DKICT Majlis Bandaraya Kuala Terengganu merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut :

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

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

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 6 of 82
MBKT, 2013			

## SKOP

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

- (a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
- (b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa, DKICT Majlis Bandaraya Kuala Terengganu ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem dan prosedur dalam pengendalian semua perkara-perkara berikut :

### (a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Majlis Bandaraya Kuala Terengganu. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

### (b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian 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 Majlis Bandaraya Kuala Terengganu;

### (c) Perkhidmatan

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

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

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 7 of 82
MBKT, 2013			

**(d) Data dan Maklumat**

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Majlis Bandaraya Kuala Terengganu. Contohnya sistem dokumentasi, prosedur operasi, rekod-rekod Majlis Bandaraya Kuala Terengganu, 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 Majlis Bandaraya Kuala Terengganu bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

**(f) Premis Komputer dan Komunikasi**

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

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

### PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT Majlis Bandaraya Kuala Terengganu 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 diberi sekiranya peranan atau fungsi pengguna memerlukan maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

**(b) Akses Minimum**

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

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 8 of 82
MBKT, 2013			

### (c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawab atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah :

- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
- iii. Menentukan maklumat sedia untuk digunakan;
- iv. Menjaga kerahsiaan kata laluan;
- v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

### (d) Pengasingan

Tugas mewujudkan, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga 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.

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 9 of 82
MBKT, 2013			

**(f) Pematuhan**

DKICT Majlis Bandaraya Kuala Terengganu hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

**(g) Pemulihan**

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

**(h) Saling Bergantungan**

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

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 10 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

<b>BIDANG 1</b>	
<b>PEMBANGUNAN DAN PENYELENGGARAAN DASAR</b>	
<b>1.1 Dasar Keselamatan ICT</b>	
<b>Objektif :</b>  Menerangkan halatuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Majlis Bandaraya Kuala Terengganu dan perundangan yang berkaitan.	
<b>1.1.1 Pelaksanaan Dasar</b>	
Pelaksanaan dasar ini akan dijalankan oleh Y.Bhg. Datuk Bandar Majlis Bandaraya Kuala Terengganu selaku Pengerusi Mesyuarat Pagi MBKT. Mesyuarat Pagi MBKT ini terdiri daripada Setiausaha Majlis dan Semua Ketua Jabatan.	Y.Bhg. Datuk Bandar Majlis Bandaraya Kuala Terengganu
<b>1.1.2 Penyebaran Dasar</b>	
Dasar ini perlu disebarikan kepada semua pengguna ICT Majlis Bandaraya Kuala Terengganu (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 11 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

---

<b>1.1.3 Penyelenggaraan Dasar</b>	
<p>DKICT Majlis Bandaraya Kuala Terengganu adalah tertakluk kepada semakan dari pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial.</p> <p>Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT Majlis Bandaraya Kuala Terengganu :</p> <ul style="list-style-type: none"><li>(a) Kenal pasti dan tentukan perubahan yang diperlukan;</li><li>(b) Kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Pagi MBKT;</li><li>(c) Maklumkan kepada semua pengguna perubahan yang telah dipersetujui oleh Mesyuarat Pagi MBKT;</li><li>(d) Dasar ini hendaklah dikaji semula sekurang-kurangnya dua tahun atau mengikut keperluan semasa.</li></ul>	ICTSO
<b>1.1.4 Pengecualian Dasar</b>	
<p>DKICT Majlis Bandaraya Kuala Terengganu adalah terpakai kepada semua pengguna ICT Majlis Bandaraya Kuala Terengganu dan tiada pengecualian diberikan.</p>	SEMUA

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 12 of 82
MBKT, 2013			

<b>BIDANG 2</b>	
<b>ORGANISASI KESELAMATAN</b>	
<b>2.1 Infrastruktur Organisasi Dalaman</b>	
<b>Objektif :</b>  Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT Majlis Bandaraya Kuala Terengganu.	
<b>2.1.1 Y.B. Datuk Bandar Majlis Bandaraya Kuala Terengganu</b>	
<p>Y.Bhg. Datuk Bandar Majlis Bandaraya Kuala Terengganu adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT Majlis Bandaraya Kuala Terengganu;</li><li>(b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT Majlis Bandaraya Kuala Terengganu;</li><li>(c) Memastikan semua keperluan organisasi (sumber kewangan sumber manusia dan perlindungan keselamatan) adalah mencukupi;</li><li>(d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT Majlis Bandaraya Kuala Terengganu; dan</li><li>(e) Mempengerusikan Mesyuarat Pagi MBKT.</li></ul>	Majlis Bandaraya Kuala Terengganu

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 13 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>2.1.2 Ketua Pegawai Maklumat (CIO)</b>	
<p>Ketua Pegawai Maklumat (CIO) bagi Majlis Bandaraya Kuala Terengganu ialah Setiausaha Majlis. Peranan dan tanggungjawab CIO adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Membantu Majlis Bandaraya Kuala Terengganu dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;</li><li>(b) Menentukan keperluan keselamatan ICT;</li><li>(c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT Majlis Bandaraya Kuala Terengganu serta pengurusan risiko dan pengauditan; dan</li><li>(d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT Majlis Bandaraya Kuala Terengganu.</li></ul>	CIO
<b>2.1.3 Pengurus ICT</b>	
<p>Pengurus ICT bagi Majlis Bandaraya Kuala Terengganu ialah Pengarah Bahagian Teknologi Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Majlis Bandaraya Kuala Terengganu;</li><li>(b) Menentukan kawalan akses pengguna terhadap aset ICT Majlis Bandaraya Kuala Terengganu;</li><li>(c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO;</li><li>(c) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Majlis Bandaraya Kuala Terengganu.</li></ul>	Pengurus ICT

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 14 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

### 2.1.4 Pegawai Keselamatan ICT

ICTSO bagi Majlis Bandaraya Kuala Terengganu ialah Penolong Pengarah Bahagian Teknologi Maklumat. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut :

ICTSO

- (a) Mengurus keseluruhan program-program keselamatan ICT Majlis Bandaraya Kuala Terengganu;
- (b) Menguatkuasakan pelaksanaan DKICT Majlis Bandaraya Kuala Terengganu;
- (c) Memberi penerangan dan pendedahan berkenaan DKICT Majlis Bandaraya Kuala Terengganu kepada semua pengguna;
- (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT Majlis Bandaraya Kuala Terengganu;
- (d) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan Majlis Bandaraya Kuala Terengganu berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
- (f) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
- (g) Melaporkan insiden keselamatan ICT KEPADA Pasukan Tindak Balas Insiden Keselamatan ICT Negeri dan memaklumpkannya kepada CIO;
- (h) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;
- (i) Menyediakan dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan
- (j) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 15 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>2.1.5 Pentadbir Sistem ICT</b>	
<p>Pentadbir sistem ICT bagi Majlis Bandaraya Kuala Terengganu ialah Penolong Pengarah Bahagian Teknologi Maklumat. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;</li><li>(b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT Majlis Bandaraya Kuala Terengganu;</li><li>(c) Memantau aktiviti capaian harian sistem aplikasi pengguna;</li><li>(d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta;</li><li>(e) Menganalisis dan menyimpan rekod jejak audit;</li><li>(f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan</li><li>(g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.</li></ul>	Pentadbir Sistem ICT
<b>2.1.6 Pengguna</b>	
<p>Pengguna mempunyai peranan dan tanggungjawab seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Membaca, memahami dan mematuhi DKICT Majlis Bandaraya Kuala Terengganu;</li></ul>	Pengguna

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 16 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"> <li>(b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;</li> <li>(c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;</li> <li>(d) Melaksanakan prinsip-prinsip DKICT Majlis Bandaraya Kuala Terengganu dan menjaga kerahsiaan maklumat Majlis Bandaraya Kuala Terengganu;</li> <li>(e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;</li> <li>(f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan</li> </ul>	
<p><b>2.2 Pihak Ketiga</b></p>	
<p><b>Objektif :</b></p> <p>Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).</p>	
<p><b>2.2.1 Keperluan Keselamatan Kontrak Dengan Pihak Ketiga</b></p>	
<p>Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal.</p> <p>Perkara yang perlu dipatuhi termasuk yang berikut :</p> <ul style="list-style-type: none"> <li>(a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Majlis Bandaraya Kuala Terengganu;</li> <li>(b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;</li> </ul>	<p>CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga</p>

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 17 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

---

- (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;
- (d) Akses kepada aset ICT Majlis Bandaraya Kuala Terengganu perlu berlandaskan kepada perjanjian kontrak;
- (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.
  - i. Dasar Keselamatan ICT Majlis Bandaraya Kuala Terengganu;
  - ii. Tapisan Keselamatan;
  - iii. Perakuan Akta Rahsia Rasmi 1972; dan
  - iv. Hak Harta Intelek.

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 18 of 82
MBKT, 2013			

<b>BIDANG 3</b>	
<b>PENGURUSAN ASET</b>	
<b>3.1 Akauntabiliti Aset</b>	
<b>Objektif :</b>  Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Majlis Bandaraya Kuala Terengganu.	
<b>3.1.1 Inventori Aset ICT</b>	
<p>Memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini;</li><li>(b) Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;</li><li>(c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di Majlis Bandaraya Kuala Terengganu;</li><li>(d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan; dan</li><li>(e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.</li></ul>	Majlis Bandaraya Kuala Terengganu

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 19 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>3.2 Pengelasan dan Pengendalian Maklumat</b>	
<b>Objektif :</b> Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
<b>3.2.1 Pengelasan Maklumat</b>	
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan.  Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut :  (a) Rahsia Besar;  (b) Rahsia;  (c) Sulit; atau  (d) Terhad.	Semua
<b>3.2.2 Pengendalian Maklumat</b>	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut :  (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;  (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;  (c) Menentukan maklumat sedia untuk digunakan;	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 20 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

---

<ul style="list-style-type: none"><li>(d) Menjaga kerahsiaan kata laluan;</li><li>(e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;</li><li>(f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan</li><li>(g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.</li></ul>	
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 21 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

---

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 22 of 82
MBKT, 2013			

## BIDANG 4

### KESELAMATAN SUMBER MANUSIA

#### 4.1 Keselamatan Sumber Manusia Dalam Tugas Harian

**Objektif :**

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

##### 4.1.1 Sebelum perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

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

Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 23 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

### 4.1.2 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut :

Semua

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

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 24 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>4.1.3 Bertukar Atau Tamat Perkhidmatan</b>	
<p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut :</p> <ul style="list-style-type: none"><li>(a) Memastikan semua aset ICT dikembalikan kepada Majlis Bandaraya Kuala Terengganu mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan</li><li>(b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Majlis Bandaraya Kuala Terengganu dan/atau terma perkhidmatan.</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 25 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

---

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 26 of 82
MBKT, 2013			

<b>BIDANG 5</b>	
<b>KESELAMATAN FIZIKAL DAN PERSEKITARAN</b>	
<b>5.1 Keselamatan Kawasan</b>	
<b>Objektif :</b>  Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
<b>5.1.1 Kawalan Kawasan</b>	
Menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi.  Perkara-perkara yang perlu dipatuhi termasuk yang 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) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;  (c) Memasang alat penggera atau kamera;  (d) Menghadkan jalan keluar masuk;  (e) Mengadakan kaunter kawalan;  (f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat;	CIO dan ICTSO

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 27 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(g) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;</li><li>(h) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;</li><li>(i) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau, dan bencana;</li><li>(j) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan</li><li>(k) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.</li></ul>	
<b>5.1.2 Kawalan Masuk Fizikal</b>	
<p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut :</p> <ul style="list-style-type: none"><li>(a) Setiap pengguna Majlis Bandaraya Kuala Terengganu hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;</li><li>(b) Semua pas keselamatan hendaklah diserahkan balik kepada Majlis Bandaraya Kuala Terengganu apabila pengguna berhenti atau bersara;</li><li>(c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan</li><li>(d) Kehilangan pas mestilah dilaporkan dengan segera kepada Majlis Bandaraya Kuala Terengganu.</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 28 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>5.1.3 Kawasan Larangan</b>	
<p>Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut.</p> <p>Kawasan larangan di Majlis Bandaraya Kuala Terengganu adalah Pusat Data :</p> <p>(a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan</p> <p>(b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.</p>	Pentadbir Sistem
<b>5.2 Keselamatan Peralatan</b>	
<b>Objektif :</b>  Melindungi peralatan ICT Majlis Bandaraya Kuala Terengganu dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
<b>5.2.1 Peralatan ICT</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <p>(a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;</p> <p>(b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;</p>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 29 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(c) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;</li><li>(d) Pengguna mestilah memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (<i>activated</i>) dan dikemaskini; di samping melakukan imbasan ke atas media storan yang digunakan;</li><li>(e) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;</li><li>(f) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;</li><li>(g) Peralatan-peralatan kritikal perlu disokong oleh <i>Uninterruptable Power Supply (UPS)</i>;</li><li>(h) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti <i>switches, hub, router</i> dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;</li><li>(i) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (<i>air ventilation</i>) yang sesuai; dan</li><li>(j) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja.</li></ul>	Semua
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 30 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

### 5.2.2 Media Storan

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CD-ROM, thumb drive dan media storan lain.

Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

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

Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 31 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>5.2.3 Media Tandatangan Digital</b>	
<p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut :</p> <ul style="list-style-type: none"><li>(a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;</li><li>(b) Media ini tidak boleh dipindah milik atau dipinjamkan;</li><li>(c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.</li></ul>	Semua
<b>5.2.4 Media perisian dan Aplikasi</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Majlis Bandaraya Kuala Terengganu;</li><li>(b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT;</li><li>(c) Lesen perisian (<i>registration code, serials, CD-Keys</i>) perlu disimpan berasingan daripada <i>CD-rom, disk</i> atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan</li><li>(d) <i>Source code</i> sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 32 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>5.2.5 Penyelenggaraan Perkakasan</b>	
<p>Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar;</li><li>(b) Memastikan perkakasan yang diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;</li><li>(c) Bertanggungjawab terhadap .setiap perkakasan bagi penyelenggaraan perkakasan samada dalam tempoh jaminan atau telah habis tempoh jaminan;</li><li>(d) Menyemak, menguji dan mengesahkan semua perkakasan sebelum dan selepas proses penyelenggaraan;</li><li>(e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan</li><li>(f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.</li></ul>	Pegawai Aset dan Bahagian Teknologi Maklumat
<b>5.2.6 Peralatan di Luar Premis</b>	
<p>Perkakasan yang dibawa keluar premis Majlis Bandaraya Kuala Terengganu adalah terdedah kepada pelbagai risiko.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan</li><li>(b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 33 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>5.2.7 Pelupusan Perkakasan</b>	
<p>Pelupusan perkakasan adalah yang melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki samada harta modal atau inventori yang dibekalkan oleh Majlis Bandaraya Kuala Terengganu.</p> <p>Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Majlis Bandaraya Kuala Terengganu.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <p>(a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah ;dihapuskan terlebih dahulu sebelum pelupusan samada melalui <i>shredding, grinding, dezauling</i> atau pembakaran;</p> <p>(b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;</p>	Semua
<p>(c) Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;</p> <p>(d) Pegawai Aset hendaklah mengenal pasti samada peralatan tertentu boleh dilupuskan atau sebaliknya;</p>	
<p>(e) Peralatan yang hendak dilupus perlu disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;</p> <p>(f) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT;</p>	
<p>(g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusatdan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan</p>	
<p>(h) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti <i>thumb drive</i> sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.</p>	

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 34 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<p>(i) Pengguna ICT adalah <b>DILARANG SAMA SEKALI</b> daripada melakukan perkara-perkara seperti berikut :</p> <ul style="list-style-type: none"> <li>i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;</li> <li>ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hard disk, motherboard dan sebagainya;</li> </ul>	Semua
<ul style="list-style-type: none"> <li>iii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Majlis Bandaraya Kuala Terengganu;</li> </ul>	
<ul style="list-style-type: none"> <li>iv. Memindah keluar dari Majlis Bandaraya Kuala Terengganu mana-mana peralatan ICT yang hendak dilupuskan; dan</li> <li>v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Majlis Bandaraya Kuala Terengganu.</li> </ul>	

### 5.3 Keselamatan Persekitaran

#### Objektif :

Melindungi aset ICT Majlis Bandaraya Kuala Terengganu dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.

#### 5.3.1 Kawalan Persekitaran

<p>Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis samada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Bahagian Teknologi Maklumat.</p> <p>Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi :</p> <ul style="list-style-type: none"> <li>(a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya)</li> </ul>	Semua
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 35 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

dengan teliti;	
(b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;	
(c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;	
(d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;	
(e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT	
(f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;	
(g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan	
(h) Akses kepada saluran <i>riser</i> hendaklah sentiasa dikunci.	

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 36 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>5.3.2 Bekalan Kuasa</b>	
<p>Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;</li><li>(b) Peralatan sokongan seperti <i>Uninterruptable Power Supply (UPS)</i> dan penjana (<i>generator</i>) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan</li><li>(c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.</li></ul>	BTM dan ICTSO
<b>5.3.3 Kabel</b>	
<p>Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah.</p> <p>Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;</li><li>(b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;</li><li>(c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan <i>wire tapping</i>; dan</li><li>(d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui <i>trunking</i> bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.</li></ul>	BTM dan ICTSO

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 37 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>5.3.4 Prosedur Kecemasan</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Setiap pengguna hendaklah membaca, memahami dan mamatuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MAMPU; dan</li><li>(b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pejabat Keselamatan Bangunan.</li></ul>	Semua
<b>5.4 Keselamatan Dokumen</b>	
<b>Objektif :</b>  Melindungi maklumat Majlis Bandaraya Kuala Terengganu dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaiian.	
<b>5.4.1 Dokumen</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;</li><li>(b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;</li><li>(c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;</li><li>(d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan</li><li>(e) Menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 38 of 82
MBKT, 2013			

<b>BIDANG 6</b>	
<b>PENGURUSAN OPERASI DAN KOMUNIKASI</b>	
<b>6.1 Pengurusan Prosedur Operasi</b>	
<b>Objektif :</b>  Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
<b>6.1.1 Pengendalian Prosedur</b>	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :  (a) Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal;  (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan  (c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Semua
<b>6.1.2 Kawalan Perubahan</b>	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :  (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 39 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<p>(b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini 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;</p> <p>(c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan</p> <p>(d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat samada secara sengaja atau pun tidak.</p>	
<p><b>6.1.3 Pengasingan Tugas dan Tanggungjawab</b></p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <p>(a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;</p> <p>(b) Tugas mewujudkan, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperinci atau dimanipulasi; dan</p> <p>(c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai <i>production</i>. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.</p>	<p>Pengurus ICT dan ICTSO</p>

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 40 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

<b>6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga</b>	
<b>Objektif :</b> Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan Pihak Ketiga.	
<b>6.2.1 Perkhidmatan Penyampaian</b>	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :  (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;  (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa ; dan  (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
<b>6.3 Perancangan dan Penerimaan Sistem</b>	
<b>Objektif :</b> Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
<b>6.3.1 Perancangan Kapasiti</b>	
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.	Pentadbir Sistem ICT dan ICTSO

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 41 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<p>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.</p>	
<b>6.3.2 Penerimaan Sistem</b>	
<p>Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.</p>	Pentadbir Sistem ICT dan ICTSO
<b>6.4 Perisian Berbahaya</b>	
<p><b>Objektif :</b></p> <p>Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.</p>	
<b>6.4.1 Perlindungan dari Perisian Berbahaya</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"> <li>(a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus. <i>Intrusion Detection System (IDS)</i> dan <i>Intrusion Prevention System (IPS)</i> serta mengikut prosedur penggunaan yang betul dan selamat;</li> <li>(b) Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997;</li> <li>(c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;</li> </ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 42 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(d) Mengemaskini antivirus dengan <i>pattern</i> antivirus yang terkini;</li><li>(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;</li><li>(f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;</li><li>(g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baikpulih sekiranya perisian tersebut mengandungi program berbahaya;</li><li>(h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan</li><li>(i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.</li></ul>	
<b>6.4.2 Perlindungan dari Mobile Code</b>	
Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
<b>6.5 Housekeeping</b>	
<b>Objektif :</b> Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 43 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>6.5.1 Backup</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Membuat <i>backup</i> keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;</li><li>(b) Membuat <i>backup</i> ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan <i>backup</i> bergantung pada tahap kritikal maklumat;</li><li>(c) Menguji sistem <i>backup</i> dan <i>prosedur restore</i> sediaada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;</li><li>(d) Menyimpan sekurang-kurangnya tiga (3) generasi <i>backup</i>; dan</li><li>(e) Merekod dan menyimpan salinan <i>backup</i> di lokasi yang berlainan dan selamat.</li></ul>	Semua
<b>6.6 Pengurusan Rangkaian</b>	
<b>Objektif :</b> Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 44 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

6.6.1 Kawalan Infrastruktur Rangkaian	
<p>Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;</li><li>(b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;</li><li>(c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;</li><li>(d) Semua peralatan mestilah melalui proses <i>Factory Acceptance Check (FAC)</i> semasa pemasangan dan konfigurasi;</li><li>(e) <i>Firewall</i> hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian ICT;</li><li>(f) Semua trafik keluar masuk hendaklah melalui <i>firewall</i> di bawah kawalan Majlis Bandaraya Kuala Terengganu;</li><li>(g) Semua perisian <i>sniffer</i> atau <i>network analyzer</i> adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;</li><li>(h) Memasang perisian <i>Intrusion Prevention System (IPS)</i> bagi mengesan sebarang cubaan mencerooboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat Majlis Bandaraya Kuala Terengganu;</li><li>(i) Memasang <i>Web Content Filtering</i> pada <i>Internet Gateway</i> untuk menyekat aktiviti yang dilarang;</li></ul>	BTM

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 45 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Majlis Bandaraya Kuala Terengganu adalah tidak dibenarkan;</li><li>(k) Semua pengguna hanya dibenarkan menggunakan rangkaian Majlis Bandaraya Kuala Terengganu sahaja dan penggunaan modem adalah dilarang sama sekali kecuali mendapat kelulusan BTM; dan</li><li>(l) Kemudahan bagi <i>wireless</i> LAN perlu dipastikan kawalan keselamatan.</li></ul>	
<b>6.7 Pengurusan Media</b>	
<b>Objektif :</b>  Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
<b>6.7.1 Penghantaran dan Pemindahan</b>	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	
<b>6.7.2 Prosedur Pengendalian Media</b>	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut : <ul style="list-style-type: none"><li>(a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;</li><li>(b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;</li><li>(c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 46 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;</li><li>(e) Menyimpan semua media di tempat yang selamat; dan</li><li>(f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.</li></ul>	
<b>6.7.3 Keselamatan Sistem Dokumentasi</b>	
<p>Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;</li><li>(b) Menyediakan dan memantapkan keselamatan sistem dokumentasi ; dan</li><li>(c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sediaada.</li></ul>	Semua
<b>6.8 Pengurusan Pertukaran Maklumat</b>	
<p><b>Objektif :</b></p> <p>Memastikan keselamatan pertukaran maklumat dan perisian antara Majlis Bandaraya Kuala Terengganu dan agensi luar terjamin.</p>	

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 47 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>6.8.1 Pertukaran Maklumat</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;</li><li>(b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara Majlis Bandaraya Kuala Terengganu dengan agensi luar;</li><li>(c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Majlis Bandaraya Kuala Terengganu; dan</li><li>(d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.</li></ul>	Semua
<b>6.8.2 Pengurusan Mel Elektronik (E-mel)</b>	
<p>Penggunaan e-mel di Majlis Bandaraya Kuala Terengganu hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan mana-mana undang-undang bertulis yang berkuat kuasa.</p> <p>Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Permohonan akaun e-mel hendaklah dibuat secara rasmi;</li><li>(b) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh Majlis Bandaraya Kuala Terengganu sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 48 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

- (c) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh Majlis Bandaraya Kuala Terengganu;
- (d) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;
- (e) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;
- (f) Penggunaan fail lampiran mestilah tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;
- (g) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;
- (h) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;
- (i) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;
- (j) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;
- (k) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;
- (l) Memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;
- (m) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 49 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

(n) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan <i>mailbox</i> masing-masing.	
<b>6.9 Perkhidmatan E-dagang (Electronic Commerce Services)</b>	
<b>Objektif :</b>  Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
<b>6.9.1 E-Dagang</b>	
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan internet.  Perkara-perkara yang perlu dipatuhi adalah seperti berikut :  (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;  (b) Maklumat yang terlibat dalam transaksi dalam talian (atas talian) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan  (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 50 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>6.9.2 Maklumat Umum</b>	
<p>Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;</li><li>(b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan</li><li>(c) memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.</li></ul>	Semua
<b>6.10 Pemantauan</b>	
<b>Objektif :</b> Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
<b>6.10.1 Pengauditan dan Forensik ICT</b>	
<p>ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut :</p> <ul style="list-style-type: none"><li>(a) Sebarang percubaan pencerobohan kepada sistem ICT Majlis Bandaraya Kuala Terengganu;</li><li>(b) Serangan kod perosak (<i>malicious code</i>), halangan pemberian perkhidmatan (<i>denial of service</i>), <i>spam</i>, pemalsuan (<i>forgery, phising</i>), pencerobohan (<i>intrusion</i>), ancaman (<i>threats</i>) dan kehilangan fizikal (<i>physical loss</i>);</li><li>(c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 51 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan luhah, berunsur fitnah dan propaganda anti kerajaan;</li><li>(e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;</li><li>(f) Aktiviti pemasangan dan penggunaan perisian yang membebankan jalur lebar (<i>bandwidth</i>) rangkaian;</li><li>(g) Aktiviti penyalahgunaan akaun e-mel; dan</li><li>(h) Aktiviti penukaran alamat IP (<i>IP address</i>) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.</li></ul>	
<b>6.10.2 Jejak Audit</b>	
<p>Setiap sistem mestilah mempunyai jejak audit (<i>audit trail</i>). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.</p> <p>Jejak audit hendaklah mengandungi maklumat-maklumat berikut :</p> <ul style="list-style-type: none"><li>(a) Rekod setiap aktiviti transaksi;</li><li>(c) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;</li><li>(c) Aktiviti capaian pengguna ke atas sistem ICT samada secara sah atau sebaliknya; dan</li><li>(d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.</li></ul>	Pentadbir Sistem ICT

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 52 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<p>Jejak Audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara.</p> <p>Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.</p>	
<b>6.10.3 Sistem Log</b>	
<p>Pentadbir sistem ICT hendaklah melaksanakan perkara-perkara berikut :</p> <ul style="list-style-type: none"><li>(a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;</li><li>(b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan</li><li>(c) Sekiranya wujud aktiviti-aktiviti yang tidak sah seperti kecurian maklumat dan pencerobohan. Pentadbir sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.</li></ul>	Pentadbir Sistem ICT
<b>6.10.4 Pemantauan Log</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;</li></ul>	Pentadbir Sistem ICT

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 53 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

---

<ul style="list-style-type: none"><li>(b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;</li><li>(c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;</li><li>(d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;</li><li>(e) Kesalahan, kesilapan dan/ atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan</li><li>(f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Majlis Bandaraya Kuala Terengganu atau <i>domain</i> keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.</li></ul>	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 54 of 82
MBKT, 2013			

<b>BIDANG 7</b>	
<b>KAWALAN CAPAIAN</b>	
<b>7.1 Dasar Kawalan Capaian</b>	
<b>Objektif :</b> Mengawal capaian ke atas maklumat	
<b>7.1.1 Keperluan Kawalan Capaian</b>	
<p>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.</p> <p>Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;</li><li>(b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;</li><li>(c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan</li><li>(d) Kawalan ke atas kemudahan pemprosesan maklumat.</li></ul>	BTM ICTSO

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 55 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

## 7.2 Pengurusan Capaian Pengguna

### Objektif :

Mengawal capaian pengguna ke atas aset ICT Majlis Bandaraya Kuala Terengganu.

### 7.2.1 Akaun Pengguna

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.

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

- (a) Akaun yang diperuntukkan oleh Majlis Bandaraya Kuala Terengganu sahaja boleh digunakan;
- (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;
- (b) Akaun pengguna yang diwujudkan akan diberi tahap capaian mengikut keperluan dan sebarang perubahan hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;
- (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Majlis Bandaraya Kuala Terengganu. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
- (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan
- (f) Pentadbir Sistem ICT boleh membeku atau menamatkan akaun pengguna atas sebab-sebab berikut :
  - i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu;
  - ii. Bertukar bidang tugas kerja;

Pemilik Sistem,  
Pentadbir  
Sistem ICT dan  
ICTSO

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 56 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"> <li>iii. Bertukar ke agensi lain;</li> <li>iv. Bersara; atau</li> <li>v. Ditamatkan perkhidmatan.</li> </ul>	
<b>7.2.2 Hak Capaian</b>	
<p>Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.</p>	<p>Pentadbir Sistem ICT</p>
<b>7.2.3 Pengurusan Kata Laluan</b>	
<p>Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Majlis Bandaraya Kuala Terengganu seperti berikut :</p> <ul style="list-style-type: none"> <li>(a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun dalam apa jua keadaan dan sebab;</li> <li>(b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;</li> <li>(c) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus;</li> <li>(d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;</li> <li>(e) Kata laluan <i>windows</i> dan <i>screen saver</i> hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;</li> </ul>	<p>Semua dan Pentadbir Sistem ICT</p>

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 57 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(f) Kata laluan hendaklah tidak dipaparkan semasa <i>input</i>, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;</li><li>(g) Kuatkuasakan pertukaran kata laluan semasa <i>login</i> kali pertama atau selepas <i>login</i> kali pertama atau selepas kata laluan diset semula;</li><li>(h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;</li><li>(i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;</li><li>(j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan</li><li>(k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.</li></ul>	
<b>7.2.4 Clear Desk dan Clear Screen</b>	
<p>Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.</p> <p><i>Clear Desk</i> dan <i>Clear Screen</i> bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada ditempatnya.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Menggunakan kemudahan <i>password screen saver</i> atau <i>logout</i> apabila meninggalkan komputer;</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 58 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<p>(b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan</p> <p>(c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.</p>	
<b>7.3 Kawalan Capaian Rangkaian</b>	
<b>Objektif :</b> Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
<b>7.3.1 Capaian Rangkaian</b>	
<p>Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan :</p> <p>(a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian Majlis Bandaraya Kuala Terengganu, rangkaian agensi lain dan rangkaian awam;</p> <p>(b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan</p> <p>(c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.</p>	Pentadbir Sistem ICT dan ICTSO

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 59 of 82
MBKT, 2013			



## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;</li><li>(i) Sebarang bahan yang dimuat dari internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Majlis Bandaraya Kuala Terengganu;</li><li>(j) Penggunaan modem untuk tujuan sambungan ke internet tidak dibenarkan sama sekali; dan</li><li>(k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut :<ul style="list-style-type: none"><li>i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet dan</li><li>ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.</li></ul></li></ul>	
<b>7.4 Kawalan Capaian Sistem Pengoperasian</b>	
<b>Objektif :</b>  Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 61 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

### 7.4.1 Capaian Sistem Pengoperasian

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

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

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

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

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

Pentadbir  
Sistem ICT dan  
ICTSO

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 62 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>7.4.2 Kad Pintar</b>			
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;</li><li>(b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;</li><li>(c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan</li><li>(d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Bahagian Teknologi Maklumat, Majlis Bandaraya Kuala Terengganu.</li></ul>			Semua
<b>7.5 Kawalan Capaian Aplikasi dan Maklumat</b>			
<b>Objektif :</b>  Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.			
<b>7.5.1 Capaian Aplikasi dan Maklumat</b>			
<p>Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.</p> <p>Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi :</p> <ul style="list-style-type: none"><li>(a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;</li></ul>			
<b>RUJUKAN</b>	<b>VERS</b>	<b>TARIKH</b>	<b>M/SURAT</b>
DKICT MBKT	Versi 1.0	30/01/2013	Page 63 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);</li><li>(c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;</li><li>(d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan</li><li>(e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimana pun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.</li></ul>	
<b>7.6 Peralatan Mudah Alih dan Kerja Jarak Jauh</b>	
<b>Objektif :</b>  Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
<b>7.6.1 Peralatan Mudah Alih</b>	
Perkara yang perlu dipatuhi adalah seperti berikut :  (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
<b>7.6.2 Kerja Jarak Jauh</b>	
Perkara yang perlu dipatuhi adalah seperti berikut :  (b) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 64 of 82
MBKT, 2013			

<h2 style="margin: 0;">BIDANG 8</h2> <h3 style="margin: 0;">PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM</h3>	
<p><b>8.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi</b></p>	
<p><b>Objektif :</b></p> <p>Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.</p>	
<p><b>8.1.1 Keperluan Keselamatan Sistem Maklumat</b></p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"> <li>(a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan yang telah disahkan dan dipersetujui bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;</li> <li>(b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan samada program berjalan dengan betul dan sempurna dan sistem <i>output</i> untuk memastikan data yang telah diproses adalah tepat;</li> <li>(c) Aplikasi perlu mengandungi semakan pengesahan <i>validation</i> untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan</li> <li>(d) Semua sistem yang dibangunkan samada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.</li> </ul>	<p>Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO</p>

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 65 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>8.1.2 Pengesahan Data Input dan Output</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <p>(a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan</p> <p>(b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.</p>	Pemilik Sistem dan Pentadbir Sistem ICT
<b>8.2 Kawalan Kriptografi</b>	
<b>Objektif :</b> Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
<b>8.2.1 Enkripsi</b>	
Pengguna hendaklah membuat enkripsi <i>encryption</i> ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
<b>8.2.2 Tandatangan Digital</b>	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
<b>8.2.3 Pengurusan Infrastruktur Kunci Awam (PKI)</b>	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 66 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

## 8.3 Keselamatan Fail Sistem

### Objektif :

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

### 8.3.1 Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

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

Pemilik Sistem dan Pentadbir Sistem ICT

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 67 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

## 8.4 Keselamatan Dalam Proses Pembangunan dan Sokongan

### Objektif :

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

### 8.4.1 Prosedur Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

- (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;
- (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh *vendor*;
- (c) Mengawal perubahan dan/ atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;
- (d) Akses kepada kod sumber *source code* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan
- (e) Menghalang sebarang bentuk ancaman yang boleh merosakkan maklumat dan aplikasi.

Pemilik Sistem dan Pentadbir Sistem ICT

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 68 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>8.4.2 Pembangunan Perisian Secara <i>Outsource</i></b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Pembangunan perisian secara <i>outsource</i> perlu diseliasa dan dipantau oleh pemilik sistem mengikut garis panduan yang; dan</li><li>(b) Kod sumber <i>source code</i> bagi semua aplikasi dan perisian adalah menjadi hak milik Majlis Bandaraya Kuala Terengganu.</li></ul>	BTM dan Pentadbir Sistem ICT
<b>8.5 Kawalan Teknikal Keterdedahan (Vulnerability)</b>	
<b>Objektif :</b>  Memastikan kawalan teknikal keterdedahan .adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesannya.	
<b>8.5.1 Kawalan dari Ancaman Teknikal</b>	
<p>Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;</li><li>(b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan</li><li>(c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.</li></ul>	Pentadbir Sistem ICT

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 69 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

---

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 70 of 82
MBKT, 2013			

<b>BIDANG 9</b>	
<b>PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN</b>	
<b>9.1 Mekanisme Pelaporan Insiden Keselamatan ICT</b>	
<b>Objektif :</b>  Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
<b>9.1.1 Mekanisme Pelaporan</b>	
<p>Insiden keselamatan ICT bermaksud musibah <i>adverse event</i> yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT samada yang ditetapkan secara tersurat atau tersirat.</p> <p>Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera :</p> <ul style="list-style-type: none"><li>(a) Maklumat didapati hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;</li><li>(b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;</li><li>(c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;</li><li>(d) Berlaku kejadian yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan</li><li>(e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.</li></ul>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 71 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<p>Prosedur pelaporan insiden keselamatan ICT berdasarkan :</p> <p>(a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan</p> <p>(c) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.</p>	
<b>9.2 Pengurusan Maklumat Insiden Keselamatan ICT</b>	
<b>Objektif :</b>  Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
<b>9.2.1 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT</b>	
<p>Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada perkhidmatan Majlis Bandaraya Kuala Terengganu.</p> <p>Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut :</p>	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 72 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

---

<ul style="list-style-type: none"><li>(a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti;</li><li>(b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;</li><li>(c) Menyediakan tindakan pemulihan segera;</li><li>(d) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu; dan</li><li>(e) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan.</li></ul>	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 73 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

---

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 74 of 82
MBKT, 2013			

<b>BIDANG 10</b>	
<b>PENGURUSAN KESINAMBUNGAN PERKHIDMATAN</b>	
<b>10.1 Dasar Kesinambungan Perkhidmatan</b>	
<b>Objektif :</b>  Memastikan operasi perkhidmatan dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
<b>10.1.1 Pelan Kesinambungan Perkhidmatan</b>	
<p>Pelan Kesinambungan Perkhidmatan - PKP) (Business Continuity Management – BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan.</p> <p>Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Mesyuarat Pagi MBKT. Perkara-perkara berikut perlu diberi perhatian :</p> <ul style="list-style-type: none"><li>(a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;</li><li>(b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;</li><li>(c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;</li><li>(d) Mendokumentasikan proses dan prosedur yang telah dipersetujui;</li></ul>	Pengurus ICT

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 75 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

- (e) Mengadakan program latihan kepada pengguna mengenal prosedur kecemasan;
- (f) Membuat backup; dan
- (g) Menguji dan mengemaskini pelan sekurang-kurangnya dua (2) tahun sekali atau mengikut keperluan semasa.

Pelan Kesyinambungan Perkhidmatan (PKP) perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut :

- (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
- (b) Senarai personel Majlis Bandaraya Kuala Terengganu dan *vendor* beserta nombor yang boleh dihubungi (*faksimile*, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan *personel* tidak dapat hadir untuk menangani insiden;
- (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
- (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
- (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan.

Salinan Pelan Kesyinambungan Perkhidmatan (PKP) perlu disimpan di lokasi utama. Salinan Pelan Kesyinambungan Perkhidmatan (PKP) hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dbangunkan.

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 76 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

---

<p>Ujian Pelan Kesenambungan Perkhidmatan (PKP) hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan <i>personel</i> yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.</p> <p>Majlis Bandaraya Kuala Terengganu hendaklah memastikan salinan Pelan Kesenambungan Perkhidmatan (PKP) sentiasa dikemaskini dan dilindungi seperti di lokasi utama.</p>	
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 77 of 82
MBKT, 2013			

# DASAR KESELAMATAN ICT MBKT

---

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 78 of 82
MBKT, 2013			

<b>BIDANG 11</b>	
<b>PEMATUHAN</b>	
<b>11.1 Pematuhan dan Keperluan Perundangan</b>	
<b>Objektif :</b>  Meningkatkan tahap keselamatan bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT Majlis Bandaraya Kuala Terengganu.	
<b>11.1.1 Pematuhan Dasar</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"><li>(a) Setiap pengguna di Majlis Bandaraya Kuala Terengganu hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT Majlis Bandaraya Kuala Terengganu dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa;</li><li>(b) Semua aset ICT di Majlis Bandaraya Kuala Terengganu termasuk maklumat yang disimpan di dalamnya adalah hak milik kerajaan. Ketua Pengarah / pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan; dan</li><li>(c) Sebarang penggunaan aset Majlis Bandaraya Kuala Terengganu selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Majlis Bandaraya Kuala Terengganu.</li></ul>	<b>SEMUA</b>

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 79 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<b>11.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal</b>	
<p>ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.</p> <p>Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.</p>	ICTSO
<b>11.1.3 Pematuhan Keperluan Audit</b>	
<p>Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.</p>	Semua
<b>11.1.4 Keperluan Perundangan</b>	
<p>Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Majlis Bandaraya Kuala Terengganu :</p> <ul style="list-style-type: none"><li>(a) Arahan Keselamatan;</li><li>(b) Pekeliling Am Bilangan 3 Tahun 2000<ul style="list-style-type: none"><li>- Rang Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;</li></ul></li><li>(c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;</li><li>(d) Peliling Am Bilangan 1 Tahun 2001<ul style="list-style-type: none"><li>- Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);</li></ul></li></ul>	SEMUA

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 80 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

- (e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003
  - 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) Surat Pekeliling Am Bilangan 4 Tahun 2006
  - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
- (h) Surat Arahan Ketua Setiausaha Negara
  - Langkah-langkah untuk memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
- (i) Surat Arahan Ketua Pengarah MAMPU
  - Langkah-langkah mengenai penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
- (j) Surat Arahan Ketua Pengarah MAMPU
  - Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
- (k) Surat Pekeliling Am Bilangan 2 Tahun 2000
  - Peranan Jawatankuasa-Jawatankuasa di bawah Jawatankuasa IT dan Internet Kerajaan (JITK);
- (l) Surat Pekeliling Perbendaharaan Bil 2/1995 (Tambahan Pertama)
  - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
- (m) Surat Pekeliling Perbendaharaan Bil 3/1995
  - Peraturan Perolehan Perkhidmatan Perundingan;
- (n) Akta Tandatangan Digital 1997;

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 81 of 82
MBKT, 2013			

## DASAR KESELAMATAN ICT MBKT

<ul style="list-style-type: none"><li>(o) Akta Rahsia Rasmi 1972;</li><li>(p) Akta Jenayah Komputer 1997;</li><li>(q) Akta Hak Cipta (Pindahan) Tahun 1997;</li><li>(r) Akta Komunikasi dan Multimedia 1998;</li><li>(s) Perintah-Perintah Am;</li><li>(t) Arahan Perbendaharaan;</li><li>(u) Arahan Teknologi Maklumat 2007;</li><li>(v) Garis Panduan Keselamatan MAMPU 2004;</li><li>(w) Standard Operating Procedure (SOP) ICT MAMPU;</li><li>(x) Surat Pekeliling Am Bilangan 3 Tahun 2009<ul style="list-style-type: none"><li>- Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;</li></ul></li><li>(y) Surat Arahan Ketua Penagarah MAMPU<ul style="list-style-type: none"><li>- Pengurusan Kesenambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.</li></ul></li></ul>	
<b>11.1.5 Pelanggaran Dasar</b>	
Pelanggaran Dasar Keselamatan ICT Majlis Bandaraya Kuala Terengganu boleh dikenakan tindakan tatatertib.	Semua

RUJUKAN	VERS	TARIKH	M/SURAT
DKICT MBKT	Versi 1.0	30/01/2013	Page 82 of 82
MBKT, 2013			