DASAR KESELAMATAN ICT

DKICT

PERBADANAN PERPUSTAKAAN AWAM TERENGGANU

VERSI 1.0

ISI KANDUNGAN **MUKA SURAT**

PENGENALAN

Dasar Keselamatan ICT (DKICT) Perbadanan Perpustakaan Awam 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 PPAT.

.

OBJEKTIF

DKICT PPAT diwujudkan untuk menjamin kesinambungan urusan PPAT dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala objektif utama keselamatan ICT PPAT ialah seperti berikut :

(a) Memastikan kelancaran operasi PPAT 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.

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 PPAT 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.

SKOP

Aset ICT Perbadanan Perpustakaan Awam Terengganu terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT PPAT 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 PPAT juga merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, dijana diwujudkan, dimusnah, disimpan, 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 Perbadanan Perpustakaan Awam Terengganu seperti 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 Perbadanan Perpustakaan Awam 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.

(d) Data dan Maklumat

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

(f) Premis Komputer dan Komunikasi

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

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT PPAT 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 mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Had akses perlu dikaji dari semasa ke semasa kepada peranan dan tanggungjawab pengguna/bidang tugas;

(c) Akauntabiliti

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

(f) Pematuhan

DKICT Perbadanan Perpustakaan Awam 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 pelan pemulihan bencana / kesinambungan perkhidmatan; dan

(h) Saling Bergantungan

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

BIDANG 1

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

1.1 Dasar Keselamatan ICT

Objektif :

Menerangkan halatuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Perbadanan Perpustakaan Awam Terengganu dan perundangan yang berkaitan.

1.1.1 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Pengarah Perbadanan Perpustakaan Awam Terengganu selaku Pengerusi Mesyuarat Pengurusan PPAT yang terdiri daripada Ketua-ketua Bahagian dan Unit.	Pengarah Perbadanan Perpustakaan Awam Terengganu

1.1.2 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna ICT PPAT (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO

1.1.3 Penyelenggaraan Dasar	
DKICT PPAT 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. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT PPAT : (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Pengurusan PPAT, (c) Maklumkan kepada semua pengguna perubahan yang dipersetujui oleh Mesyuarat Pengurusan PPAT; dan (d) Dasar ini hendaklah dikaji semula sekurang-kurangnya dua tahun atau mengikut keperluan semasa.	ICTSO
1.1.4 Pengecualian Dasar	
DKICT Perbadanan Perpustakaan Awam Terengganu terpakai kepada semua pengguna ICT PPAT dan tiada pengecualian diberikan.	SEMUA

BIDANG 2

ORGANISASI KESELAMATAN

2.1 Infrastruktur Organisasi Dalaman

Objektif :

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT PPAT. .

2.1.1 Pengarah Perbadanan Perpustakaan Awam Terengganu

Pengarah Perbananan Perpustakaan Awam Terengganu adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut : (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT PPAT ; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT Perbadanan Perpustakaan Awam Terengganu; (c) Memastikan semua keperluan organisasi (sumber Kewangan sumber manusia dan perlindungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT PPAT; dan (e) Mempengerusikan Mesyuarat Pengurusan PPAT	Perbadanan Perpustakaan Awam Terengganu

2.1.2 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) bagi PPAT ialah Ketua Bahagian Khidmat Pengurusan. Peranan dan tugas bagi CIO adalah seperti berikut : (a) Membantu dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan keselamatan ICT; (c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT PPAT serta pengurusan risiko dan pengauditan; dan (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT PPAT.	CIO
2.1.3 Pengurus ICT	
Pengurus ICT bagi PPAT ialah Ketua Unit Teknologi Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut : (a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan PPAT; (b) Menentukan kawalan akses pengguna terhadap aset ICT Perbadanan Perpustakaan Awam Terengganu; (c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; (c) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Perbadanan Perpustakaan Awam Terengganu	Pengurus ICT

2.1.4 Pegawai Keselamatan ICT

ICTSO bagi Perbadanan Perpustakaan Awam Terengganu ialah Penolong Pegawai Teknologi Maklumat. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut : (a) Mengurus keseluruhan program-program keselamatan ICT Perbadanan Perpustakaan Awam Terengganu; (b) Menguatkuasakan pelaksanaan DKICT Perbadanan Perpustakaan Awam Terengganu; (c) Memberi penerangan dan pendedahan berkenaan DKICT Perbadanan Perpustakaan Awam Terengganu kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT Perbadanan Perpustakaan Awam Terengganu; (d) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan Perbadanan Perpustakaan Awam 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 memaklumkannya 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.	ICTSO

2.1.5 Pentadbir Sistem ICT	
Pentadbir sistem ICT bagi Perbadanan Perpustakaan Awam Terengganu Pegawai Teknologi Maklumat. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut : (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT PPAT; (c) Memantau aktiviti capaian harian sistem aplikasi pengguna; (d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; (e) Menganalisis dan menyimpan rekod jejak audit; (f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan (g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	Pentadbir Sistem ICT
2.1.6 Pengguna	
Pengguna mempunyai peranan dan tanggungjawab seperti berikut : (a) Membaca, memahami dan mematuhi DKICT PPAT;	Pengguna

(b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; (d) Melaksanakan prinsip-prinsip DKICT Perbadanan Perpustakaan Awam Terengganu dan menjaga kerahsiaan maklumat Perbadanan Perpustakaan Awam Terengganu; (e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan	
2.2 Pihak Ketiga	
Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
2.2.1 Keperluan Keselamatan Kontrak Dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut : (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Perbadanan Perpustakaan Awam Terengganu; (b) Mengenal pasti risko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

(c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;

(d) Akses kepada aset ICT PPAT 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 Perbadanan Perpustakaan Awam Terengganu;

ii. Tapisan Keselamatan;

iii. Perakuan Akta Rahsia Rasmi 1972; dan

iv. Hak Harta Intelek.

BIDANG 3

PENGURUSAN ASET

3.1 Akauntabiliti Aset

Objektif :

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Perbadanan Perpustakaan Awam Terengganu.

3.1.1 Inventori Aset ICT

Memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini; (b) Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di Perbadanan Perpustakaan Awam Terengganu; (d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan; dan (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Perbadanan Perpustakaan Awam Terengganu

3.2 Pengelasan dan Pengendalian Maklumat

Objektif :

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

3.2.1 Pengelasan Maklumat

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

3.2.2 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan;	Semua

(d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

BIDANG 4

KESELAMATAN SUMBER MANUSIA

4.1 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif :

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan Perb. Perpustakaan Awam Terengganu pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna ICT PPAT 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 Perb. Perpustakaan Awam Terenggan serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan Perb. Perpustakaan Awam 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

4.1.2	**Dalam Perkhidmatan**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut : (a) Memastikan pegawai dan kakitangan Perb. Perpustakaan Awam Terengganu serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Perb. Perpustakaan Awam Terengganu; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT Perb. Perpustakaan Awam 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 Per. Perpustakaan Awam Terengganu serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh Perb. Perpustakaan Awam 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. Pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan PPAT bagi sebarang kursus dan latihan teknikal yang diperlukan,	Semua

4.1.3	**Bertukar Atau Tamat Perkhidmatan**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut : (a) Memastikan semua aset ICT dikembalikan kepada Perbadanan Perpustakaan Awam Terengganu mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Perb. Perpustakaan Awam Terengganu dan/atau terma perkhidmatan.	Semua

BIDANG 5

KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.1 Keselamatan Kawasan

Objektif :

Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

5.1.1 Kawalan Kawasan

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

(g) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (h) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (i) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau, dan bencana; (j) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (k) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
5.1.2 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut : (a) Setiap pelawat Perb. Perpustakaan Awam Terengganu hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan balik kepada Perb. Perpustakaan Awam Terengganu apabila pengguna berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan segera kepada Perbadanan Perpustakaan Awam Terengganu.	Semua

5.1.3 Kawasan Larangan	
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. Kawasan larangan Perpustakaan Awam Negeri Terengganu adalah Pusat Data : (a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan (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.	Pentadbir Sistem
5.2 Keselamatan Peralatan	
Objektif : Melindungi peralatan ICT Perb. Perpustakaan Awam Terengganu dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
5.2.1 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;	Semua

(c) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (d) Pengguna mestilah memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini; di samping melakukan imbasan ke atas media storan yang digunakan; (e) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (f) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (g) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (*UPS*); (h) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (i) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; dan (j) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja.	Semua

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

5.2.3	**Media Tandatangan Digital**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut : (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Semua
5.2.4	**Media perisian dan Aplikasi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Perb. Perpusakaan Awam Terengganu; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (c) Lesen perisian (*registration code, serials, CD-Keys*) perlu disimpan berasingan daripada *CD-rom, disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua

5.2.5	**Penyelenggaraan Perkakasan**	
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan yang diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap .setiap perkakasan bagi penyelenggaraan perkakasan samada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak, menguji dan mengesahkan semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	Pegawai Aset dan Unit Teknologi Maklumat
5.2.6	**Peralatan di Luar Premis**	
	Perkakasan yang dibawa keluar premis PPAT adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua

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

(i) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut : i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hard disk, motherboard dan sebagainya;	Semua
iii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Perbadanan Perpustakaan Awam Terengganu;	
iv. Memindah keluar dari Perb. Perpustakaan Awam Terengganu mana-mana peralatan ICT yang hendak dilupuskan; dan v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Perb. Perpustakaan Awam Terengganu.	

5.3 Keselamatan Persekitaran

Objektif :

Melindungi aset ICT Perb. Perpustakaan Awam Terengganu dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

5.3.1 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis samada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Unit Teknologi Maklumat. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi : (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya)	Semua

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 *riser* hendaklah sentiasa dikunci.	

5.3.2	**Bekalan Kuasa**	
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (*UPS*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	UTM dan ICTSO
5.3.3	**Kabel**	
	Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	UTM dan ICTSO

	5.3.4 Prosedur Kecemasan	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Setiap pengguna hendaklah membaca, memahami dan mamatuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MAMPU; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Unit Selenggara.	Semua
5.4	**Keselamatan Dokumen**	
	Objektif : Melindungi maklumat Perb. Perpustakaan Awam Terengganu dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
	5.4.1 Dokumen	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (e) Menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua

BIDANG 6

PENGURUSAN OPERASI DAN KOMUNIKASI

6.1 Pengurusan Prosedur Operasi

Objektif :

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

6.1.1 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Semua prosedur pengurusan operasi yang diwujud, 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 pemprosesaan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Semua

6.1.2 Kawalan Perubahan

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

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

6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif :

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan Pihak Ketiga.

6.2.1 Perkhidmatan Penyampaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Memastikan kawalan keselamatan, definasi 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

6.3 Perancangan dan Penerimaan Sistem

Objektif :

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

6.3.1 Perancangan Kapasiti

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

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.	
6.3.2 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT dan ICTSO
6.4 Perisian Berbahaya	
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.	
6.4.1 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus. *Intrusion Detection System* (*IDS*) dan *Intrusion Prevention System* (*IPS*) serta mengikut posedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;	Semua

(d) Mengemaskini antivirus dengan *pattern* antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baikpulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
6.4.2 Perlindungan dari Mobile Code	
Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
6.5 Housekeeping	
Objektif : Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	

6.5.1 *Backup*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurannya sekali atau setelah mendapat versi terbaru; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; (c) Menguji sistem *backup* dan *prosedur restore* sediada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan (e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Semua
6.6 Pengurusan Rangkaian	
Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	

6.6.1	**Kawalan Infrastruktur Rangkaian**	
	Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (*FAC*) semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian ICT; (f) Semua trafik keluar masuk hendaklah melalui *firewall* di bawah kawalan Perbadanan Perpustakaan Awam Terengganu; (g) Semua perisian *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; (h) Memasang perisian *Intrusion Prevention System* (*IPS*) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat Perb. Perpustakaan Awam Terengganu; (I) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;	UTM

(j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Perb. Perpustakaan Awam Terengganu adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian Perb. Perpustakaan Awam Terengganu sahaja dan penggunaan modem adalah dilarang sama sekali kecuali mendapat kelulusan UTM; dan (l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	

6.7 Pengurusan Media

Objektif :

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

6.7.1 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.

6.7.2 Prosedur Pengendalian Media

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut : (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;	Semua

(d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; dan (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
6.7.3 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut : (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyediakan dan memantapkan keselamatan sistem dokumentasi ; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sediada.	Semua
6.8 Pengurusan Pertukaran Maklumat	
Objektif : Memastikan keselamatan pertukaran maklumat dan perisian antara Perbadanan Perpustakaan Awam Terengganu dan agensi luar terjamin.	

6.8.1	**Pertukaran Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian diantara PPAT dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari PPAT; dan (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
6.8.2	**Pengurusan Mel Elektronik (E-mel)**	
	Penggunaan e-mel Perb. Perpustakaan Awam 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. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut : (a) Permohonan akaun e-mel hendaklah dibuat secara rasmi; (b) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh Perbadanan Perpustakaan Awam Terengganu sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;	Semua

(c) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh Perbadanan Perpustakaan Awam 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 dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan

(n) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	

6.9 Perkhidmatan E-dagang (Electronic Commerce Services)

Objektif :

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

6.9.1 E-Dagang

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

6.9.2 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut : (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua
6.10 Pemantauan	
Objektif : Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
6.10.1 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut : (a) Sebarang percubaan pencerobohan kepada sistem ICT Perbadanan Perpustakaan Awam Terengganu; (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); (c) Pengubahsuain ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;	Semua

(d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti pemasangan dan penggunaan perisian yang membebankan jalur lebar (*bandwith*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	
6.10.2 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). 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. Jejak audit hendaklah mengandungi maklumat-maklumat berikut : (a) Rekod setiap aktiviti transaksi; (c) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT samada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.	Pentadbir Sistem ICT

Jejak Audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. 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.	
6.10.3 Sistem Log	
Pentadbir sistem ICT hendaklah melaksanakan perkara-perkara berikut : (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti yang tidak sah seperti kecurian maklumat dan pencerobohan. Pentadbir sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT
6.10.4 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk temph masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;	Pentadbir Sistem ICT

(b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (e) Kesalahan, kesilapan dan/ atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan (f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Per. Perpustakaan Awam Terengganu atau *domain* keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

BIDANG 7

KAWALAN CAPAIAN

7.1 Dasar Kawalan Capaian

Objektif :

Mengawal capaian ke atas maklumat

7.1.1 Keperluan Kawalan Capaian

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. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	UTM ICTSO

7.2 Pengurusan Capaian Pengguna

Objektif :

Mengawal capaian pengguna ke atas aset ICT Perb. Perpustakaan Awam 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 Perb. Perpustakaan Awam Terengganusahaja 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 Perb. Perpustakaan Awam 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

iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
7.2.2 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
7.2.3 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Perb. Perpustakaan Awam Terengganu seperti berikut : (a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun dalam apa jua keadaan dan sebab; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus; (d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;	Semua dan Pentadbir Sistem ICT

(f) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; (g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; (j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan (k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
7.2.4 *Clear* Desk dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada ditempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;	Semua

(b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	

7.3 Kawalan Capaian Rangkaian

Objektif :

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

7.3.1 Capaian Rangkaian

Kawalan capaian perkhidatan rangkaian hendaklah dijamin selamat dengan : (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian Perbadanan Perpustakaan Awam Terengganu rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem ICT dan ICTSO

7.3.2	**Capaian Internet**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut :	Pentadbir Rangkaian
	(a) Penggunaan internet Perbadanan Perpustakaan Awam Terengganu hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, *virus* dan bahan-bahan yang tidak sepatutnya di dalam rangkaian Perb. Perpustakaan Awam Terengganu;	
	(b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	
	(c) Penggunaan teknologi *packet shaper* untuk mengawal aktiviti *video conferencing*, *video streaming*, *chat*, *downloading* adalah perlu bagi menguruskan penggunaan jalur lebar *bandwith* yang maksimum dan lebih berkesan;	Pentadbir Rangkaian
	(d) Penggunaan internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya;	Rangkaian
	(e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah / pegawai yang diberi kuasa;	Semua
	(f) Bahan yang diperolehi dari internet hendaklah ditentukan ketetapan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber internet hendaklah dinyatakan ;	
	(g) Bahan rasmi hendaklah disemak dan disahkan sebelum dimuat naik ke internet;	

(h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

(i) Sebarang bahan yang dimuat dari internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Perb. Perpustakaan Awam Terengganu;

(j) Penggunaan modem untuk tujuan sambungan ke internet tidak dibenarkan sama sekali; dan

(k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut :

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

ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

7.4 Kawalan Capaian Sistem Pengoperasian

Objektif :

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

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 perlanggaran 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

7.4.2	**Kad Pintar**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; (b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (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 (d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Unit Teknologi Maklumat, Perbadanan Perpustakaan Awam Terengganu.	Semua
7.5	**Kawalan Capaian Aplikasi dan Maklumat**	
	Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
7.5.1	**Capaian Aplikasi dan Maklumat**	
	Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi : (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;	

(b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimana pun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	

7.6 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif :

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

7.6.1 Peralatan Mudah Alih

Perkara yang perlu dipatuhi adalah seperti berikut : (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua

7.6.2 Kerja Jarak Jauh

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

BIDANG 8

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

8.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif :

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

8.1.1 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (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 menggangu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan samada program berjalan dengan betul dan sempurna dan sistem *output* untuk memastikan data yang telah diproses adalah tepat; (c) Aplikasi perlu mengandungi semakan pengesahan *validation* untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (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.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

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

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

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

8.4.2 Pembangunan Perisian Secara *Outsource*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Pembangunan perisian secara outsource perlu diselia dan dipantau oleh pemilik sistem mengikut garis panduan yang; dan (b) Kod sumber *source code* bagi semua aplikasi dan perisian adalah menjadi hak milik Perbadanan Perpustakaan Awam Terengganu.	UTM dan Pentadbir Sistem ICT
8.5 Kawalan Teknikal Keterdedahan (Vulnerability)	
Objektif : Memastikan kawalan teknikal keterdedahan .adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
8.5.1 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

BIDANG 9

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

9.1 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif :

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

9.1.1 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah *adverse event* 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. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera : (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; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; (d) Berlaku kejadian yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	Semua

Prosedur pelaporan insiden keselamatan ICT berdasarkan : (a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (c) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	

9.2 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif :

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

9.2.1 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianlisis 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 Perbadanan Perpustakaan Awam Terengganu 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 :	Semua

(a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan tindakan pemulihan segera; (d) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu; dan (e) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan.	

BIDANG 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

10.1 Dasar Kesinambungan Perkhidmatan

Objektif :

Memastikan operasi perkhidmatan dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

10.1.1 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan - PKP) (Business Continuity Management – BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Mesyuarat Pengurusan PPAT. Perkara-perkara berikut perlu diberi perhatian : (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (d) Mendokumentasikan proses dan prosedur yang telah dipersetujui;	Pengurus ICT

(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 keperluaan semasa.

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

(a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

(b) Senarai personel Perb. Perpustakaan Awam 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 Kesinambungan Perkhidmatan (PKP) perlu disimpan di lokasi utama. Salinan Pelan Kesinambungan 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.

Ujian Pelan Kesinambungan Perkhidmatan (PKP) hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan *personel* yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. Perbadanan Perpustakaan Awam Terengganu hendaklah memastikan salinan Pelan Kesinambungan Perkhidmatan (PKP) sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	

BIDANG 11

PEMATUHAN

11.1 Pematuhan dan Keperluan Perundangan

Objektif :

Meningkatkan tahap keselamatan bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT Perbadanan Perpustakaan Awam Terengganu.

11.1.1 Pematuhan Dasar

Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Setiap pengguna di Perbadanan Perpustakaan Awam Terengganu hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT Perb. Perpustakaan Awam Terengganu dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa; (b) Semua aset ICT di Perbadanan Perpustakaan Awam 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 (c) Sebarang penggunaan aset Perb. Perpustakaan Awam Terengganu selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Perbadanan Perpustakaan Awam Terengganu.	SEMUA

11.1.2	**Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal**	
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.	ICTSO
11.1.3	**Pematuhan Keperluan Audit**	
	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.	Semua
11.1.4	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Perbadanan Perpustakaan Awam Terengganu: (a) Arahan Keselamatan; (b) Pekeliling Am Bilangan 3 Tahun 2000 - Rang Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; (c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002; (d) Peliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);	Semua

(e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003
- Garis Panduan Mmengenai 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;

(o) Akta Rahsia Rasmi 1972; (p) Akta Jenayah Komputer 1997; (q) Akta Hak Cipta (Pindahan) Tahun 1997; (r) Akta Komunikasi dan Multimedia 1998; (s) Perintah-Perintah Am; (t) Arahan Perbendaharaan; (u) Arahan Teknologi Maklumat 2007; (v) Garis Panduan Keselamatan MAMPU 2004; (w) Standard Operating Procedure (SOP) ICT MAMPU; (x) Surat Pekeliling Am Bilangan 3 Tahun 2009 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009; (y) Surat Arahan Ketua Penagarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.	
11.1.5 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT Perb. Perpustakaan Awam Terengganu boleh dikenakan tindakan tatatertib.	Semua

	Glosari
Antivirus	Perisian yang mengimbas virus pada media storan, seperti cakera keras (hard disk) dan disket (diskette) untuk sebarang kemungkinan adanya virus
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
Aset ICT	Peralatan ICT termasuk komputer, media storan, server, router, firewall, rangkaian dan lain-lain.
Backup	Proses penduaan sesuatu dokumen atau maklumat
Bandwidth	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi dalam jangka
CIO	Chief Information Officer
Denial of Service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan. Proses enkripsi data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
ICT	Information and Communication Technology
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
PKI	Public-Key Infrastructure Infrastruktur Kunci Awam
Server	Pelayan
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.