DKICT

DASAR KESELAMATAN ICT DBKL

DEWAN BANDARAYA KUALA LUMPUR

No. Dokumen	DKICT-ISMS-DBKL-01
No. Keluaran	03
No. Pindaan	00
Tarikh Kuatkuasa	2 Januari 2020

Disediakan Oleh :

.....

Nama : Nor Eyniwati Binti Hassan
Jawatan : Pengarah
Jabatan Pengurusan Maklumat
Tarikh : 30 Disember 2019

Diluluskan Oleh :

.....

Nama : Dato' Nor Hisham Bin A Dahlan
Jawatan : Datuk Bandar
Tarikh : 02 Januari 2020

DASAR KESELAMATAN ICT DBKL

ISO/IEC 27001:2013

DEWAN BANDARAYA KUALA LUMPUR,
MENARA DBKL 1,
JALAN RAJA LAUT,
50350 KUALA LUMPUR
TEL:03-26179000

Laman Web:http://www.dbkl.gov.my

	DASAR KESELAMATAN ICT (DKICT)	No. Dokumen: DKICT-ISMS-DBKL-01
		No.Keluaran: 03
		No. Pindaan: 00
	DEWAN BANDARAYA KUALA LUMPUR	Muka Surat: **i** dari **77**
		Tarikh Kuat Kuasa : 2 Januari 2020

REKOD PINDAAN DOKUMEN

NO. KELUARAN	TARIKH KUAT KUASA PINDAAN	BAB / MUKA SURAT	PERKARA YANG DIPINDA	KETERANGAN RINGKAS MENGENAI PINDAAN
01	18 Nov 2013	Semua	Pindaan keseluruhan dokumen	Penambahbaikan Dokumen
02	1 Julai 2017	Semua	Pindaan keseluruhan dokumen	Penambahbaikan Dokumen
03	2 Januari 2020	Semua	Pindaan keseluruhan dokumen	Penambahbaikan Dokumen

KANDUNGAN

PENGENALAN

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

OBJEKTIF

Dasar Keselamatan ICT DBKL diwujudkan untuk menjamin kesinambungan urusan DBKL dengan meminimumkan kesan insiden keselamatan ICT.
Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi DBKL. Ini hanya boleh dicapai dengan memastikan aset ICT dilindungi.
Manakala, objektif utama Keselamatan ICT DBKL ialah seperti berikut:

a. Memastikan kelancaran operasi DBKL 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 DBKL.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.
Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a. Melindungi maklumat rahsia rasmi dan maklumat rasmi DBKL dari capaian tanpa kuasa yang sah;
b. Menjamin setiap maklumat adalah tepat dan sempurna;
c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

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

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

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

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

SKOP

Aset ICT terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT DBKL 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. Data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan DBKL, perkhidmatan dan pelanggan.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT DBKL ini merangkumi perlindungan bentuk maklumat DBKL yang

dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian perkara-perkara berikut:

a. Perkakasan

Aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

b. Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada DBKL;

c. Perkhidmatan

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

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

d. Data atau Maklumat

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

f. Premis Komputer Dan Komunikasi

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

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

PRINSIP-PRINSIP

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

1. **Akses atas dasar perlu mengetahui**
   Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Garis Panduan Keselamatan DBKL.

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

3. **Akauntabiliti**
   pengguna adalah dipertanggungjawabkan ke atas 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 dipertanggungjawabkan 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.

4. Pengasingan

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

5. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

6. Pematuhan

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

7. 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

8. 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.

- BIDANG 01 -

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

PERKARA	**TANGGUNGJAWAB**
BIDANG 01 – PEMBANGUNAN DAN PENYELENGGARAAN DASAR	
0101 Dasar Keselamatan ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan fungsi-fungsi utama DBKL dan perundangan yang berkaitan.	
010101 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh Datuk Bandar DBKL dan dibantu oleh Pengarah Eksekutif dan Pengarah Jabatan.	Datuk Bandar Kuala Lumpur
010102 Penyebaran Dasar	
Dasar ini hendaklah disebarkan dan dipatuhi oleh pengguna aset ICT DBKL (DBKL) termasuk pihak ketiga yang berurusan atau memberikan perkhidmatan ICT kepada DBKL.	CIO
010103 Penyelenggaraan Dasar	
Dasar ini hendaklah disemak sekurang-kurangnya sekali setahun dan dipinda mengikut keperluan selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial.	ICTSO
010104 Pengecualian Dasar	
Dasar ini adalah terpakai kepada pengguna ICT DBKL termasuk pihak ketiga dan tiada pengecualian diberikan.	CIO

- BIDANG 02 -

ORGANISASI KESELAMATAN

BIDANG 02 - ORGANISASI KESELAMATAN

0201 Organisasi DBKL

Objektif:
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT DBKL.

020101 Datuk Bandar DBKL

Datuk Bandar DBKL adalah berperanan dan bertanggungjawab dalam perkara-perkara berikut: a) Meluluskan dokumen Dasar Keselamatan ICT (DKICT) DBKL; b) Meluluskan struktur dan fungsi Jawatankuasa Keselamatan ICT; c) Meluluskan keperluan sumber berasaskan kepada dasar dan peraturan semasa;dan d) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) DBKL.	Datuk Bandar DBKL

020102 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) bagi DBKL ialah Pengarah Eksekutif (Pengurusan) **Peranan dan tanggungjawab CIO adalah seperti berikut:** a) Membantu Datuk Bandar dalam melaksanakan tugas-tugas yang melibatkan ICT dan keselamatan ICT; b) Meluluskan prosedur, standard, dan garispanduan keselamatan ICT DBKL; c) Meluluskan perlaksanaan atau aktiviti keselamatan ICT DBKL; d) Menentukan keperluan keselamatan ICT; e) Meluluskan pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT DBKL serta pengurusan risiko dan pengauditan; f) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT DBKL; g) Bertanggungjawab keseluruhan program-program keselamatan ICT DBKL; h) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT DBKL; dan i) Bertanggungjawab ke atas Pengurusan Kesinambungan Perkhidmatan DBKL.	CIO

020103 Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT (ICTSO) bagi DBKL ialah Pengarah Jabatan Pengurusan Maklumat. **Peranan dan tanggungjawab ICTSO adalah seperti berikut:** a) Mengurus keseluruhan program-program keselamatan ICT DBKL; b) Melaksanakan Dasar Keselamatan ICT DBKL; c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT DBKL kepada pengguna; d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT DBKL; e) Menjalankan pengurusan risiko; f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan DBKL berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h) Melaporkan insiden keselamatan ICT kepada kepada CIO; i) Bekerjasama dengan pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; k) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan l) Koordinator Pengurusan Kesinambungan Perkhidmatan ICT (Koordinator PKPICT) DBKL.	ICTSO

020104 Pengurus ICT

Pengurus ICT bagi DBKL ialah Timbalan Pengarah, Bahagian Pengurusan Infrastruktur ICT, Jabatan Pengurusan Maklumat. **Peranan dan tanggungjawab Pengurus ICT yang dilantik adalah seperti berikut:**	Pengurus ICT

a) Mentadbir dan mengurus operasi ICT DBKL; b) Mengkaji, menguji dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan DBKL; c) Membuat penilaian keberkesanan kawalan keselamatan ICT; d) Meluluskan prosedur teknikal perlaksanaan kawalan keselamatan; e) Menentukan kawalan akses pengguna terhadap aset ICT DBKL; f) Memastikan dasar keselamatan ICT dipatuhi; g) Mengambil tindakan terhadap pencerobohan, ancaman atau penemuan mengenai kelemahan keselamatan ICT; h) Menyediakan pelaporan insiden keselamatan ICT kepada kepada ICTSO; dan i) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT DBKL.	
020105 Pentadbir Sistem ICT	
Pentadbir Sistem ICT bagi DBKL ialah Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai Teknologi Maklumat/Penolong Jurutera merupakan Pentadbir Sistem ICT di DBKL. **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 Dasar Keselamatan ICT DBKL; 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; g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, computer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	Pentadbir Sistem ICT (Aplikasi, Multimedia, Server dan Rangkaian)

020106 Personel DBKL	
Personel DBKL adalah kakitangan yang dilantik oleh Datuk Bandar secara tetap, kontrak dan sambilan. **Personel mempunyai peranan dan tanggungjawab seperti berikut:** a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT DBKL; 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 Dasar Keselamatan ICT DBKL dan menjaga kerahsiaan maklumat DBKL; e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;dan f) Menghadiri program-program kesedaran mengenai keselamatan ICT.	Personel DBKL
020107 Jawantankuasa Pemandu ICT DBKL (JPICT)	
a) Menetapkan arah tuju dan strategi untuk pelaksanaan ICT; b) Menentukan kaedah pelaksanaan projek secara inhouse atau outsourcing; c) Merancang dan menyelaras pelaksanaan program/projek ICT; d) Menyelaras dan menyeragamkan pelaksanaan ICT DBKL agar selari dengan Pelan Strategik ICT DBKL dan Pelan Strategik ICT Sektor Awam; e) Meluluskan projek ICT dan bajet; f) Mengikuti dan memantau perkembangan program ICT serta memahami keperluan, menyelesaikan masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT; dan g) Merancang dan menentukan langkah-langkah keselamatan ICT.	JPICT
020108 Jawantakuasa Teknikal ICT (JTICT)	
a) Menganalisa, memberi penyelesaian dan pengesyoran untuk pelaksanaan ICT di DBKL; b) Memantau pelaksanaan program/projek-projek ICT agar selari dengan Pelan Strategik ICT DBKL dan Pelan Strategik ICT	JTICT

Sektor Awam; c) Mengemukakan laporan dan pengesyoran ke JPICT DBKL untuk kelulusan; d) Membuat keputusan kaedah perolehan; e) Mengikuti perkembangan program ICT serta memahami keperluan, menyelesaikan masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT dan mengesyorkan langkah-langkah keselamatan ICT; f) Meluluskan tahap pematuhan keselamatan ICT; g) Meluluskan skop pensijilan ISMS; h) Meluluskan penemuan awal penilaian risiko aset ICT; i) Meluluskan pengurusan dokumen dan rekod perlaksanaan ISMS; j) Meluluskan teknologi yang besesuaian untuk dilaksanakan di dalam memperkukuhkan keselamatan ICT; k) Meluluskan cadangan penyelesaian terhadap keperluan keselamatan ICT dan insiden ICT; l) Memastikan DKICT DBKL selaras dengan dasar-dasar ICT kerajaan semasa; m) Meluluskan laporan dan membincangkan hal-hal keselamatan ICT semasa; n) Meluluskan tindakan yang melibatkan pelanggaran DCIKT DBKL; dan o) Meluluskan tindakan yang perlu diambil mengenai sebarang insiden.	
020109 Pasukan Tindak Balas Insiden Keselamatan ICT DBKL	
Pasukan tindak balas insiden keselamatan ICT DBKL adalah pasukan yang akan bertindak semasa berlaku insiden keselamatan di DBKL. Pasukan terdiri daripada Pengurus ICT dan Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai Teknologi Maklumat/Penolong Jurutera. Pengguna wajib melaporkan sebarang insiden ICT kepada pasukan tindak balas insiden keselamatan ICT DBKL mengikut prosedur yang ditetapkan apabila berlaku insiden yang menjejaskan keselamatan ICT **Peranan dan tanggungjawab Pasukan adalah seperti berikut :** a) Menerima dan mengesan aduan keselamatan ICT serta menilai	Pasukan Tindak Balas Insiden Kelamatan ICT DBKL

tahap dan jenis insiden; b) Merekod dan menjalankan siasatan awal insiden yang diterima; c) Menangani tindak balas (response) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d) Menasihati CIO mengambil tindakan pemulihan dan pengukuhan; e) Memberikan khidmat nasihat dan amaran awal insiden; dan f) Menyebarkan maklumat berkaitan pengukuhan keselamatan ICT kepada pihak yang berkepentingan.	
0202 Pihak Ketiga	
Objektif: Menjamin keselamatan aset ICT yang digunakan Pembekal, Kontraktor, Pakar Runding dan lain-lain adalah terkawal keselamatannya dan tidak disalahguna.	
020201 Keperluan Keselamatan ICT di dalam Kontrak dengan Pihak Ketiga	
Perjanjian kontrak dengan pihak ketiga yang berurusan dengan aset ICT perlu memastikan penggunaan maklumat dan kemudahan proses maklumat dikawal. **Perkara yang perlu dipatuhi di dalam perjanjian adalah seperti berikut:** a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT DBKL; b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Akses kepada aset ICT DBKL perlu berlandaskan kepada perjanjian kontrak; e) Memastikan syarat-syarat keselamatan dan prosedur dipatuhi dan dinyatakan dengan jelas kepada pihak ketiga; f) Memastikan Hak Harta Intelek dilindungi; dan g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT DBKL sebagaimana **Lampiran 1.**	Pihak Ketiga

- BIDANG 03 -

PENGURUSAN ASET

BIDANG 03 - PENGURUSAN ASET

0301 Tanggungjawab Terhadap Aset

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

030101 Inventori Aset ICT

Ini bertujuan memastikan aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. **Perkara yang perlu dipatuhi adalah seperti berikut:** a) Memastikan aset ICT dikenal pasti dan maklumat aset direkod dan dikemas kini; b) Memastikan maklumat penyelenggaraan aset ICT direkod dan sentiasa dikemas kini; c) Memastikan aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; d) Memastikan pengguna mengesahkan penempatan aset ICT yang ditempatkan di DBKL; e) Memastikan pegerakan dan peminjaman aset ICT direkod dan dipantau; f) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; g) Setiap pengguna adalah bertanggungjawab ke atas aset ICT di bawah kawalannya; dan h) Peraturan bagi pengendalian pelupusan aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan.	Pegawai Aset setiap Jabatan

0302 Pengelasan dan Pengendalian Maklumat

Objektif:
Memastikan setiap maklumat diberikan tahap perlindungan yang bersesuaian.

030201 Pengelasan Maklumat

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut Garis Panduan Keselamatan DBKL. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan seperti berikut:	Pegawai Rekod setiap Jabatan

a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad.	
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan ; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua Personel

- BIDANG 04 -

KESELAMATAN SUMBER MANUSIA

BIDANG 04 - KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia

Objektif:
Memastikan personel DBKL, pembekal, kontraktor, pakar runding dan lain-lain memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Personel DBKL hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

040101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menjalankan tapisan keselamatan untuk personel DBKL dan 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; dan b) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua Jabatan

040102 Semasa Perkhidmatan

Objektif:
Memastikan personel DBKL dan pihak ketiga mempunyai kesedaran terhadap ancaman keselamatan dan sedar akan tanggungjawab bagi memastikan segala dasar keselamatan dilaksanakan di dalam kerja yang dilakukan untuk menurunkan risiko akibat kesilapan manusia.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan DBKL yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Memastikan personel DBKL serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh DBKL; c) Memastikan latihan kesedaran atau yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT DBKL secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;	Semua Jabatan

d) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas personel DBKL sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh DBKL; dan e) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	
040103 Tamat Perkhidmatan atau Pertukaran Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan aset ICT dikembalikan kepada DBKL mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan, menggantung atau menarik balik kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh DBKL dan/atau terma perkhidmatan.	Jabatan Pengurusan Sumber Manusia dan; Semua Jabatan

- BIDANG 05 -

KESELAMATAN FIZIKAL DAN PERSEKITARAN

BIDANG 05 - KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

Objektif:
Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

050101 Keselamatan Kawasan Fizikal

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi (bergantung kepada hasil penilaian risiko) termasuk yang berikut : a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset; 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; g) Mewujudkan perkhidmatan kawalan keselamatan; h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; j) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau dan bencana; k) Menyediakan garis panduan untuk personel yang bekerja di kawasan terhad; dan l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Jabatan Pentadbiran

050102 Kawalan Masuk Fizikal	
Kawalan Masuk Fizikal perlu dikenal pasti dan dilaksanakan ke atas kawasan yang menempatkan infrastruktur rangkaian dan komunikasi, fasiliti pemprosesan atau tempat penyimpanan maklumat terperingkat. Keselamatan fizikal termasuk keselamatan perimeter seperti pembinaan dinding, pagar kawalan dan menghadkan jalan keluar masuk ke kawasan berkenaan. Akses ke kawasan pejabat dan kawasan larangan perlu dikawal bagi memastikan hanya personel atau pihak yang diberi tanggungjawab sahaja dibenarkan masuk.	Semua Jabatan
050103 Kawasan Larangan ICT	
Kawasan larangan ditakrifkan sebagai kawasan dimana terdapat aset ICT kritikal yang boleh menjejaskan operasi dan keselamatan maklumat secara keseluruhan jika tidak dikawal. Kawasan larangan ICT di DBKL ialah Bilik UPS, Bilik Main Distribution Frame (MDF), Pusat Data (Data Centre), Bilik Toner, Bilik Pendaftaran Rahsia, Bilik Media dan Bilik Staging. Akses kepada kawasan larangan hendaklah dikawal dan kebenaran hanyalah kepada personel yang dibenarkan sahaja; dan pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan aktiviti mereka hendaklah dipantau atau diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Semua Jabatan
050104 Perlindungan Kawasan ICT dari ancaman luar dan bencana alam	
Kawalan dan perlindungan keselamatan ke atas kawasan yang mempunyai Aset ICT perlu mengambilkira ancaman dari perbuatan manusia ataupun bencana alam seperti kebakaran, banjir, gempa bumi dan lain-lain.	Semua Jabatan

050105 Kawalan Kawasan Penghantaran Barangan dan *Loading Area*	
Kawasan penghantaran barangan dan *loading area* hendaklah dikawal dan perlu dipisahkan dari akses terus ke kawasan larangan.	Jabatan Pentadbiran
0502 Keselamatan Aset ICT	
Objektif: Melindungi aset ICT dari kehilangan, kerosakan, kecurian aset serta gangguan kepada aset tersebut.	
050201 Peralatan dan Perkakasan ICT	
Aset ICT perlu dijaga dan dikawal dengan baik supaya ianya boleh digunakan sepanjang masa, perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Pengguna hendaklah menyemak dan memastikan aset 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; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini disamping melakukan imbasan ke atas media storan yang digunakan; g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h) Peralatan sokongn ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterrutable Power Supply* (UPS); j) 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	Semua

perlu diletakkan di dalam rak khas dan berkunci; k) Peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation)* yang sesuai; l) Peralatan ICT yang hendak dibawa keluar dari premis DBKL perlulah mendapat kelulusan oleh pegawai yang diberikan kuasa dan direkodkan bagi tujuan pemantauan; m) Peralatan ICT yang hilang hendaklah dilaporkan kepada Unit Pengurusan Aset dan Fasiliti Jabatan Pentadbiran, ICTSO dan Pegawai Aset Jabatan dengan segera serta laporan polis hendaklah disertakan; n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT dan pegawai aset DBKL; p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; q) Sebarang pelekat selain tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; t) Pengguna bertanggungjawab terhadap perkakasan, perisisan dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; u) Pengguna hendaklah memastikan perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF” apabila meninggalkan pejabat; v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan w) Memastikan suis ditutup bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
050202 Media Storan Digital	
Media storan digital merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cekera padat, pita	Semua

magnetik, *optical disk, flash disk*, CDROM, *thumb drive* dan media storan lain. Media storan digital perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti yang 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) Media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d) 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 atau pendua (backup) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h) 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.	
050203 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti 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; dan c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan selanjutnya.	Semua Jabatan

050204 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan DBKL; b) Sistem aplikasi dalaman tidak dibenarkan didemostrasi atau diagih kepada pihak lain kecuali dengan kebenaran ICTSO; c) Lesen perisian 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 pindaaan mestilah mengikut prosedur yang ditetapkan.	Semua Jabatan
050205 Utiliti Sokongan	
Utiliti sokongan perlu berada dalam keadaan terbaik dan mencukupi bagi menyokong sistem beroperasi. Utiliti sokongan ini termasuk bekalan elektrik, air, penghawa dingin, generator, alat komunikasi dan lain-lain.	Unit Penyelenggaraan Bangunan, Jabatan Pelaksanaan Projek dan Penyelenggaraan Bangunan.
050206 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti adalah terkawal. Perkara-perkara yang perlu dipatuhi termasuk yang tersenarai di bawah: a) Perkakasan perlu diselenggara mengikut spesifikasi yang telah ditetapkan oleh pengeluar; b) Memastikan perkakasan hanya boleh diselenggara oleh personel atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan	Jabatan Pengurusan Maklumat dan semua Jabatan

f) Penyelenggaraan mestilah mendapat kebenaran daripada pegawai yang diberikan tanggungjawab menjaganya.	
050207 Aset ICT di Luar Premis	
Aset ICT seperti storan penyimpanan maklumat, komputer peribadi, komputer tablet, telefon mudah alih, *smart card*, dokumen atau lain-lain perkakasan yang berada di luar premis DBKL perlu dilindungi dari risiko keselamatan seperti kecurian, kerosakan dan lain-lain. Antara perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Aset yang hendak dibawa keluar dari premis perlu mendapat kebenaran; b) Pegawai adalah bertanggungjawab sepenuhnya ke atas aset yang dibawa keluar; c) Aset perlu dilindungi dan dikawal sepanjang masa; d) Penyimpanan atau penempatan aset mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua Jabatan
050208 Pelupusan dan Guna Semula Perkakasan	
Pelupusan melibatkan aset ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh DBKL dan ditempatkan di DBKL. Aset ICT yang akan dilupuskan atau diguna semula, terutama yang mengandungi maklumat terperingkat atau perisian yang dilesenkan, perlu diuruskan dengan teratur dan selamat mengikut prosedur pelupusan semasa atau guna semula peralatan yang telah ditetapkan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan DBKL. **Perkara-perkara yang perlu dipatuhi adalah seperti berikut:** a) Kandungan perkakasan khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan atau diguna semula; b) Pelupusan Aset ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa. c) Kandungan peralatan khususnya maklumat rahsia rasmi	Semua Jabatan

hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran atau kaedah lain yang bersesuaian;

d) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat pendua;

e) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

f) Pegawai Aset Jabatan hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

g) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

h) Pegawai Aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori;

i) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

j) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;

ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian DBKL;

iii. Memindah keluar dari DBKL mana-mana peralatan ICT yang hendak dilupuskan;

iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Bahagian Pentadbiran Jabatan; dan

v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

0503 Keselamatan Persekitaran

Objektif:
Melindungi aset ICT DBKL dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan**.**

050301 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada ICTSO. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi : a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik pencetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti. b) 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 bersesuaian dan berjauhan dari aset ICT; e) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; f) Cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; g) Peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya sekali (1) kali dalam setahun. Aktiviti dan keputusan ujian ini pelu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	Semua Jabatan

050302 Bekalan Kuasa

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.	Jabatan Pelaksanaan Projek dan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Peralatan ICT kritikal 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)* hendaklah digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan c) Peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Penyelenggaraan Bangunan
050303 Kabel	
Kabel rangkaian hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : a) Menggunakan kabel yang mengikuti 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) Kabel perlu dilabelkan dengan jelas dan melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Jabatan Pengurusan Maklumat
050304 Prosedur Kecemasan Persekitaran	
Prosedur kecemasan persekitaran seperti kebakaran, banjir, bencana alam dan lain-lain yang melibatkan persekitaran kawasan ICT terjejas hendaklah di kaji dari masa ke semasa. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut : a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Manual Keselamatan Bangunan Menara 1, Menara 2 dan Menara 3 DBKL; dan	Semua Jabatan

b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) dan Penolong Pegawai Keselamatan Jabatan.	
0504 Keselamatan Dokumen	
Objektif: Melindungi maklumat DBKL dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut : a) Dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terhad, Sulit, Rahsia atau Rahsia Besar; b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; c) Kehilangan dan kerosakan ke atas jenis dokumen perlu dimaklumkan mengikut Prosedur Arahan Keselamatan; dan d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa sepertimana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara.	Semua

- BIDANG 06 -
PENGURUSAN OPERASI DAN KOMUNIKASI

BIDANG 06 - PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur Operasi dan Tanggungjawab

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

060101 Pengendalian Prosedur Operasi ICT

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) 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; dan c) Prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan dan diberikan nombor versi pindaan dan diluluskan oleh ICTSO.	Semua

060102 Kawalan Perubahan

Perubahan yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah dikemukakan oleh Pemilik Sistem atau Pentadbir Sistem ICT dan mendapat kebenaran daripada pegawai yang diberi kuasa; dan Sebarang perubahan komponen sistem ICT hendaklah mematuhi keperluan yang ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Pengubahsuaian yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan	Semua

d) Aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Pengasingan Tugas dan Tanggungjawab	
Tugas dan tanggungjawab setiap pegawai perlu ditetapkan dan jelas bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT. 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, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c) Perkakasan yang digunakan bagi membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production.* Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	ICTSO ,Pengurus ICT
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif: Memastikan penyampaian perkhidmatan pihak ketiga mematuhi tahap keselamatan yang ditetapkan selaras dengan perjanjian perkhidmatan.	
060201 Perkhidmatan	
Pihak ketiga perlu mematuhi terma dan syarat-syarat berkaitan kawalan keselamatan yang telah ditetapkan dalam perjanjian perkhidmatan. Perkara-perkara yang mesti dipatuhi seperti berikut : a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;	Semua

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.	
060202 Pemantauan Perkhidmatan Pihak Ketiga	
Perkhidmatan, laporan dan rekod pihak ketiga perlu dipantau, disemak dan diaudit.	Pentadbir Sistem ICT
0603 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 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. Keperluan kapasiti ini juga perlu mangambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT, ICTSO
060302 Penerimaan Sistem	
Sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Perakuan penerimaan sistem hanya akan dikeluarkan setelah segala ujian penerimaan yang ditetapkan berjaya dilaksanakan sepenuhnya.	Pentadbir Sistem ICT, ICTSO

0604 Kawalan Terhadap Perisian Berbahaya

Objektif:
Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.

060401 Perlindungan Dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Instrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; c) Mengimbas perisian atau sistem dengan anti virus sebelum menggunakannya; d) Mengemaskini anti virus 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 baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Semua

060402 Kawalan terhadap kod berbahaya (*Malicious Code)*

Perisian atau sistem yang digunakan mesti bebas daripada kod berbahaya (*malicious code)*	Semua

060403 Kawalan terhadap *Mobile Code*

Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua

0605 Housekeeping (back up)

Objektif:
Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

060501 Back-up dan Restore

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah mengikut prosedur yang telah ditetapkan. Perkara-perkara yang perlu dicontohi adalah seperti berikut : a) Membuat *backup* keselamatan ke atas sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat *backup* ke atas data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c) Menguji sistem *backup* dan *restore* sedia ada 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.	ICTSO; Pengurus ICT; dan Pentadbir Sistem ICT.

0606 Pengurusan Keselamatan Rangkaian

Objektif:
Memastikan maklumat dan infrastruktur rangkaian dilindungi.

060601 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 yang 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	ICTSO; Pengurus ICT; dan Pentadbir Rangkaian.

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) Peralatan mestilah lulus proses *Factory Acceptance Check* (FAC) dan ujian piawaian yang ditetapkan oleh SIRIM atau agensi piawaian antarabangsa semasa dikeluarkan serta lulus Final Acceptance Test setelah pemasangan dan konfigurasi;

e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian;

f) Trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan DBKL;

g) Perisian *sniffer* atau *network analyser* 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 DBKL;

i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan DBKL adalah tidak dibenarkan;

k) Pengguna hanya dibenarkan menggunakan rangkaian DBKL sahaja dan penggunaan *modem* persendirian adalah dilarang sama sekali;

l) Peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai antivirus yang sah;

m) Capaian kepada rangkaian perlu dilaksanakan mengikut kategori yang telah ditetapkan iaitu intranet, internet dan DMZ;

n) Sistem yang terdapat di dalam rangkaian intranet tidak dibenarkan dicapai dari internet;

o) Pihak ketiga adalah tidak dibenarkan untuk mencapai rangkaian intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran pemilik sistem; dan

p) Capaian kepada wireless hendaklah dikawal mengikut kategori pengguna.

0607 Pengendalian Media

Objektif:
Melindungi media mudah alih dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan perkhidmatan.

060701 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu dan perlu mematuhi prosedur yang ditetapkan.	Semua

060702 Prosedur Pengendalian Dan Pelupusan Media

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut :

a) Melabelkan 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;
d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;
e) Menyimpan 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.

060703 Keselamatan Sistem Dokumentasi

Sistem dokumentasi perlu disimpan dengan selamat dan dilindungi daripada capaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem didokumentasi adalah seperti berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan	Semua

c) Mengawal dan merekodkan aktiviti capaian dokumentasi sedia ada.	
0608 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara DBKL dan agensi luar terjamin.	
060801 Pertukaran Maklumat	
Pertukaran maklumat mesti mendapat kelulusan dari pihak pengurusan. 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 di antara DBKL dengan agensi luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari DBKL; dan d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya. (emel encrpytion)	Semua
060802 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel hendaklah mamatuhi kod etika, garis panduan dan peraturan yang ditetapkan oleh DBKL. Di antara perkara yang perlu dipatuhi oleh pengguna e-mail DBKL ialah: a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukan oleh DBKL boleh digunakan semasa membuat urusan rasmi; b) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; c) Pengguna perlu memastikan saiz email yang dihantar tidak melebihi saiz yang ditetapkan oleh penerima; d) Pengguna tidak dibenarkan menghantar lampiran (*attachment*)	Semua

melebihi had yang ditetapkan; e) Pengguna bertanggungjawab membuat salinan atau *backup* e-mail; f) Pengguna hendaklah menyemak dan menentukan tarikh dan masa sistem komputer adalah sentiasa tepat; g) Pengguna perlu memastikan e-mail dibaca dan diambil tindakan segera; h) Pengguna perlu memastikan *mailbox* mempunyai ruangan storan yang cukup terutama untuk transaksi di hujung minggu atau cuti ;dan i) Pengguna bertanggungjawab mengemaskini *mailbox* masing-masing.	
060803 Business Information System	
Maklumat yang terlibat dalam perkongsian data di antara sistem aplikasi perlu dilindungi.	Semua
0609 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.	
060901 E-Dagang	
Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan. Perkhidmatan E-dagang melalui kemudahan Internet adalah dibenarkan dengan kawalan bagi menjamin keselamatan maklumat. 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 (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan	Pengurus ICT; dan Pentadbir Sistem ICT

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.	
060902 Transaksi atas talian	
Maklumat yang terlibat dalam transaksi atas talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian dan pendedahan yang tidak dibenarkan.	Pemilik Sistem dan Pentadbir Sistem ICT
060903 Maklumat Capaian Umum	
Maklumat yang dipaparkan perlu mempunyai tahap integriti yang tinggi dan dilindungi dari pindaan yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti yang 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.	Pentadbir Sistem ICT
0610 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061001 Pengauditan dan Forensik ICT	
Pentadbir Sistem mestilah bertanggungjawab mengesan, merekod dan menganalisis perkara-perkara berikut : a) Sebarang percubaan pencerobohan kepada sistem ICT DBKL; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*deniel of service*), spam, pemalsuan (*forgery phising*), pencerobohan (*instrusion*), ancaman (*threats*) dan	Pentadbir Sistem ICT

kehilangan fizikal (*physical loss*); c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; 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 instalasi dan penggunaan perisian yang membebankan jalur lebar *(bandwitdth*) 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.	
061002 Jejak Audit	
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; b) 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 sama ada secara sah atau sebaliknya; dan d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa tidak kurang dari setahun atau yang ditetapkan pihak pengurusan atau peraturan semasa. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT

061003 Sistem Log	
Bagi memastikan aktiviti sistem dipantau, Pentadbir Sistem ICT perlu melaksanakan perkara-perkara berikut : a) Mewujudkan sistem log bagi merekodkan 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
061004 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Log Audit yang merekodkan aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan 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 DBKL atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pentadbir Sistem ICT
061008 Penyeragaman Waktu	
Sistem ICT DBKL perlu mempunyai waktu yang seragam dengan *Network Time Protokol* (NTP) DBKL.	Pentadbir Sistem

- BIDANG 07 -

KAWALAN CAPAIAN

BIDANG 07 - KAWALAN CAPAIAN

0701 Kawalan Capaian

Objektif:
Memastikan capaian kepada maklumat adalah berdasarkan kepada keperluan organisasi dan keselamatan maklumat.

070101 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini 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 server; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Kawalan ke atas kemudahan pemprosesan maklumat mengikut keperluan keselamatan dan peranan pengguna.	Pentadbir Sistem ICT

0702 Pengurusan Capaian Pengguna

Objektif:
Mengawal capaian pengguna ke atas aset ICT DBKL.

070201 Pendaftaran Akaun Pengguna

Pendaftaran, pengemaskinian dan penamatan akaun penguna mestilah dilaksanakan mengikut prosedur yang ditetapkan. 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 pengguna hanya diwujudkan setelah mendapat pengesahan Ketua Jabatan Pemohon dan pemilik sistem ICT serta pengguna telah mengesahkan memahami Dasar Keselamatan ICT. b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c) Sebarang perubahan tahap capaian hendaklah mendapat	Semua

kelulusan daripada Ketua Jabatan Pemohon dan pemilik sistem ICT terlebih dahulu; d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan DBKL. Akaun boleh ditarik balik jika penggunaanya melanggar peraturan; e) Penggunaan akaun milik orang lain adalah dilarang; f) Penggunaan akaun tidak boleh dikongsi; dan g) Akaun pengguna boleh dibeku atau ditamatkan apabila menerima arahan daripada Ketua Jabatan Pemohon dan pemilik sistem ICT	
070202 Hak Capaian *(priviledge)*	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pemilik Sistem, Pentadbir Sistem ICT
070203 Semakan Hak Capaian Pengguna	
Pemilik sistem perlu menyemak hak capaian pengguna dari masa ke semasa bagi memastikan tiada berlaku penyalahgunaan hak capaian.	Pemilik Sistem Pentadbir Sistem ICT
070204 Pengurusan Kata Laluan Pengguna	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta garis panduan yang ditetapkan oleh DBKL. Penggunaan ***default administrator*** dan **guest** adalah tidak dibenarkan.	Pentadbir Sistem ICT
0703 Tanggungjawab Pengguna	
Objektif: Menghalang capaian yang tidak dibenarkan terhadap maklumat dan fasiliti pemprosesan.	
070301 Penggunaan Akaun dan Kata Laluan	
Capaian kepada sistem ICT DBKL perlu mempunyai akaun pengenalan diri dan kata laluan. Antara perkara yang perlu dipatuhi ialah:	Semua

a) Penggunaan akaun ***administrator*** adalah dilarang; b) *System administrator* yang dilantik perlu menggunakan akaun sendiri tetapi mempunyai capaian sebagai *administrator* kecuali di dalam keadaan yang tertentu atas kebenaran CIO/ICTSO; c) Salinan akaun dan kata laluan *administrator* hendaklah disimpan oleh ICTSO dan jika berlaku pertukaran katalaluan, salinan tersebut perlu dikemaskini; d) Pengguna tidak dibenarkan menggunakan akaun pengguna lain; e) Pengguna perlu menukar kata laluan secara berkala; dan f) Pengguna perlu mematuhi amalan terbaik keselamatan ICT dalam pemilihan dan penggunaan kata laluan.	
070302 *Unattended user equipment*	
Peralatan ICT yang diletakkan berjauhan dari pemilik/pengguna atau ditinggalkan bersendiriaan perlu mematuhi perkara-perkara berikut: a) Komputer yang *idle* dalam tempoh 15 minit akan di *lock screen*; b) peralatan ICT perlu *log off* setelah tugasan selesai; dan c) Kawalan yang bersesuaian perlu dilaksanakan bagi peralatan tanpa pengawasan.	Semua
070303 *Clear Desk dan Clear Screen*	
Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. a) Pengguna perlu *lock screen* apabila meninggalkan komputer pada bila-bila masa, jika tidak screen akan di*lock*/*hibernate* selepas 15 minit idle; b) Fail atau dokumen terperingkat perlu disimpan di tempat yang berkunci apabila meninggalkan meja kerja; c) Maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan; dan d) Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; ii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan iii. Memastikan dokumen diambil segera dari pencetak,	Semua

pengimbas, mesin faksimili (jika berkaitan) dan mesin fotostat.	
070304 Penggunaan Komputer	
Penggunaan aset komputer DBKL termasuk desktop *dan notebook* perlu dikawal supaya tiada pencerobohan, penyalahgunaan, kecurian, kehilangan dan pengubahsuaian kepada maklumat.	
Pengguna komputer DBKL perlu mematuhi perkara berikut: a) Komputer DBKL hendaklah digunakan untuk tugas rasmi sahaja; b) Pengguna bertanggungjawab memastikan bahawa komputer perlu sentiasa mempunyai *antivirus* yang aktif dan terkini; c) Komputer perlu didaftar pemiliknya dan pemilik berkenaan adalah bertanggungjawab menjaga keselamatan komputer tersebut sehingga komputer tersebut dilupuskan; d) Ketua Bahagian adalah bertanggungjawab terhadap komputer gunasama, dan setiap pergerakkan komputer tersebut perlu direkodkan; e) Pegawai yang dibekalkan dengan *notebook*, komputer tablet dan *smart phone* dibenarkan untuk membawa pulang atau dibawa ke mana-mana dan pegawai adalah bertanggungjawab menjaga keselamatan aset berkenaan sepanjang masa; f) Pentadbir Sistem berhak untuk menyiasat kandungan mana-mana kategori komputer apabila menerima arahan daripada CIO atau ICTSO secara jarak jauh (*remote*) atau mendapatkan komputer tersebut dari pengguna; g) Komputer milik DBKL adalah dilarang digunakan oleh pihak ketiga tanpa kawalan dan pengawasan pegawai DBKL; dan h) Pegawai perlu melaporkan dengan segera sekiranya berlaku kehilangan komputer, notebook, komputer tablet atau *smart phone* kepada DBKL dengan menyertakan salinan laporan Polis.	Semua
0704 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas perkhidmatan Rangkaian (wayar dan tanpa wayar) DBKL.	
070401 Capaian Rangkaian	
Penggunaan perkhidmatan rangkaian diberikan kepada pengguna berasaskan kepada tugas dan skop kerja. Sistem/aplikasi atau	Semua

pengguna perlu mematuhi kawalan capaian perkhidmatan rangkaian yang ditetapkan seperti berikut; a) Capaian akan berasaskan kepada 3 zone rangkaian iaitu internet, intranet, demilitarized zone (DMZ) da; b) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian DBKL, rangkaian agensi lain dan rangkaian awam; c) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunanya; d) Menghalang mana-mana pengguna awam memasuki ke rangkaian intranet tanpa pengawasan; e) Kontraktor atau pihak ketiga adalah dilarang membawa keluar peralatan yang digunakan untuk mencapai rangkaian intranet kecuali telah mendapat pengesahan pemilik sistem; dan f) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
070402 Capaian Internet	
Capaian melalui internet (Rangkaian Awam) kepada rangkaian dan maklumat DBKL hendaklah dikawal bagi memastikan tiada berlaku kecurian, pencerobohan, kerosakan dan pengubahsuaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Hanya aplikasi yang berada di dalam DMZ zone saja dibenarkan dicapai melalui internet. b) Pengguna berdaftar DBKL adalah dibenarkan untuk mencapai rangkaian internet dengan kawalan berasaskan tugas-tugas rasmi dan skop kerja. c) Capaian ke Intranet DBKL menggunakan internet atau rangkaian awam adalah tidak dibenarkan; d) Penggunaan Internet di DBKL hendaklah dipantau secara berterusan bagi memastikan penggunaanya untuk tujuan capaian yang dibenarkan sahaja seperti yang terdapat di dalam tatacara penggunaan internet; e) Penggunaan *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; f) Aktiviti (*video conferencing*, *video streaming, chat*, *downloading*) perlu dikawal bagi menguruskan penggunaan jalur lebar	Pentadbir Rangkaian Pengurus ICT

(*bandwidth)* yang maksimum dan lebih berkesan kecuali untuk kegunaan rasmi; g) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja, CIO berhak menentukan penggunaan yang dibenarkan atau sebaliknya; h) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Datuk Bandar atau CIO ; i) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Jabatan sebelum dimuat naik ke Internet; j) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; k) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh DBKL; l) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board atau* sebagainya. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; m) Penggunaan modem/broadband pada mana-mana peralatan atau aset yang berada atau bersambung dengan rangkaian DBKL adalah dilarang sama sekali kerana ianya akan menjadi *backdoor* kepada rangkaian DBKL; dan n) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut; i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan eletronik, 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.	
070403 Peralatan Dalam Rangkaian	
Bagi memastikan bahawa peralatan yang disambungkan kepada Rangkaian DBKL tidak menjejaskan keselamatan maklumat dan capaian, maka perkara-perkara berikut hendaklah dipatuhi:	Pentadbir Rangkaian

a) Peralatan perlu disahkan bebas daripada virus dan perisian antivirus hendaklah dipasang dan masih aktif sepanjang masa; b) Hanya peralatan yang telah berdaftar dibenarkan di sambungan *(join)* kepada rangkaian; c) Setiap peralatan yang hendak disambung ke rangkaian perlu menggunakan protocol TCP/IP dan akan menggunakan *IP address* dan *domain name* yang ditetapkan oleh pentadbir rangkaian; dan d) Konfigurasi peralatan dalam rangkaian selepas daripada *Switches* adalah menjadi tanggungjawab pengguna.	
070404 Capaian ke atas Port untuk Tujuan Diagnostik	
Bagi memastikan bahawa port rangkaian tidak dicapai tanpa pengawasan, perkara berikut perlu dipatuhi oleh pengguna; a) Port yang tidak digunakan perlu *disable*; b) Capaian fizikal dan logikal ke atas port untuk tujuan diagnostik perlu mendapat kebenaran pegawai yang diberikan kuasa; c) Capaian oleh pegawai DBKL hanya dibenarkan berasaskan kepada tugas dan skop kerja; dan d) Capaian oleh pihak ketiga perlu mendapat kelulusan dari pegawai yang diberikan kuasa.	Pentadbir Rangkaian
070405 Pengasingan Dalam Rangkaian	
Rangkaian DBKL perlu dibuat pengasingan menggunakan VLAN, Zone (Intranet, DMZ, Internet) dan VPN mengikut jenis perkhidmatan, pengguna, sensitiviti maklumat dan sistem.	Pentadbir Rangkaian
070406 Kawalan Penghalaan *(Routing)* Rangkaian	
Penghalaan perlu dikawal supaya ianya tidak disalah guna dengan memastikan perkara berikut: a) Konfigurasi routing perlu disemak, disahkan dan diluluskan oleh peringkat pegawai-pegawai yang berlainan yang diberi kuasa sebelum dilaksanakan; b) Semakan *routing table* perlu dibuat dari masa ke semasa; dan c) Penghalaan (Routing) di dalam sistem rangkaian perlu dilaksanakan dengan betul dan terkawal.	Pentadbir Rangkaian

0705 Kawalan Capaian Sistem Pengoperasian

Objektif:
Menghalang capaian yang tidak sah dan tanpa dibenarkan ke atas sistem pengoperasian.

070501 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 mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan; b) Mewujudkan jejak audit ke atas capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan Perkara-perkara yang perlu dipatuhi adalah seperti yang 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 program; dan d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	Pentadbir Sistem

070502 Secure Log-on

Log-on ke atas sistem pengoperasian perlu melalui satu kaedah yang selamat bagi mengurangkan akses yang tidak dibenarkan.	Pentadbir Sistem

070503 Pengenalan dan Pengesahan pengguna

Capaian masuk sistem perlu mempunyai kaedah bagi mengenal dan mengesahkan pengguna adalah sah.	Pentadbir Sistem

070504 Penggunaan Sistem Utiliti	
Penggunaan sistem utiliti perlulah dikawal dan dihad kepada pegawai yang dibenarkan saja.	Pentadbir Sistem ICT
070505 Session Time-Out	
Sesi yang tidak aktif perlu ditamatkan mengikut tempoh masa sekurang-kurangnya 10 minit atau tempoh yang bersesuaian.	Pentadbir Sistem ICT
0706 Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
070601 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 diberikan 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 bagaimanapun, penggunaanya terhad kepada perkhidmatan yang dibenarkan sahaja. f) Had masa capaian kepada maklumat dan sistem aplikasi hendaklah berasaskan kepada keperluan dan fungsi pengguna;	Semua

dan g) Masa capaian bagi aplikasi *social networking* dibenarkan pada waktu rehat 1:00 ptg – 2:00 ptg dan selepas waktu pejabat 5.30 ptg – 7.00 malam (Isnin-Jumaat).	
070602 Larangan Capaian Maklumat	
Capaian kepada maklumat perlu dikawal bagi memastikan integriti, kerahsiaan dan kecapaian sentiasa terjamin. Antara perkara perlu dipatuhi ialah : a) Capaian kepada maklumat dan sistem aplikasi hendaklah berasaskan kepada keperluan dan fungsi pengguna; b) Capaian kepada maklumat yang tidak rasmi, berunsur lucah, iklan dan yang menjejaskan prestasi kerja adalah dilarang.	Semua
070603 Pengasingan Sistem Kritikal	
Sistem yang mendatangkan risiko yang tinggi kepada operasi DBKL perlu di asingkan daripada capaian terus melalui internet. Pengasingan kepada sistem-sistem ini perlu dilaksana dengan menggunakan VLAN/VPN dan zon rangkaian (intranet, DMZ, Internet)	Pentadbir Sistem ICT
0707 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
070701 Peralatan Mudah Alih	
Peralatan mudah alih ICT ialah peralatan yang mudah dibawa ke mana-mana dan mempunyai capaian kepada rangkaian internet atau data. Perkara yang perlu dipatuhi adalah seperti berikut : a) Peralatan mudah alih yang dikhaskan untuk pegawai yang berkelayakan dibenarkan dibawa keluar bagi melaksanakan tugas-tugas rasmi; b) Peralatan mudah alih gunasama perlu direkod dan mendapat kelulusan pegawai yang bertanggungjawab apabila hendak	Semua

dibawa keluar dari pejabat; c) Peralatan mudah alih hendaklah dilindungi dan dikawal dengan selamat; dan d) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	
070702 Kemudahan Kerja Jarak Jauh	
Kerja Jarak Jauh hanya boleh dilaksanakan setelah disemak dan mendapat kelulusan pegawai yang diberi kuasa dan pemilik sistem yang berkaitan. Perkara yang perlu dipatuhi adalah seperti berikut : a) Hanya peralatan mudah alih milik DBKL saja boleh digunakan untuk mencapai maklumat dan sistem aplikasi di dalam Rangkaian Intranet DBKL; b) Pegawai yang bukan kakitangan DBKL adalah tidak dibenarkan kecuali untuk tujuan khidmat sokongan yang akan dipantau oleh pegawai DBKL sepanjang masa aktiviti tersebut dilaksanakan dan aktiviti tersebut perlu direkod mengikut prosedur dan garispanduan yang ditetapkan; c) Capaian jarak jauh yang berada di dalam zon intranet hendaklah menggunakan *Virtual Private Network* (VPN); d) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Pentadbir Sistem

- BIDANG 08 -

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

BIDANG 08 - PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif

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

080101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh menggangu pemprosesan dan ketetapan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas sistem dan input data untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem dan *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) Sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. e) Pihak ketiga adalah tertakluk kepada perjanjian *Non Disclosure Agreement* (NDA) bagi penggunaan data sebenar (*operational data*) pada persekitaran pengujian atau *Proof of Concept* (POC).	Pentadbir Sistem ICT; Pemilik Sistem, Pihak Ketiga.

080102 Analisa Dan Spesifikasi Keperluan Keselamatan

Spesifikasi reka bentuk perlu memasukkan keperluan keselamatan sistem maklumat. Sekiranya sesuatu *off-the-shelves* produk diperolehi, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.	Pentadbir Sistem ICT

0802 Kebolehpercayaan Pemprosesan Dalam Aplikasi	
Objektif: Untuk mengelak kesalahan, kecacatan, kerugian, pengubahsuaian yang tidak dibenarkan, penyalahgunaan maklumat dalam aplikasi atau kehilangan kepercayaan terhadap sistem.	
080201 Pengesahan Data *Input*	
Data yang dimasukkan ke dalam aplikasi perlu disahkan untuk memastikan data adalah tepat dan betul.	Pemilik Sistem
080202 Kawalan Bagi Pemprosesan Dalaman	
Satu prosedur pengujian perlu diwujudkan di dalam aplikasi bagi mengesan sebarang kerosakan maklumat yang terhasil dari kesilapan dan kecacatan pemprosesan ataupun kesalahan yang disengajakan. Aktiviti-aktiviti pengujian didokumenkan dan hasil keputusan perlu disimpan dengan selamat.	Pentadbir Sistem ICT
080203 Integriti Maklumat	
Satu penilaian terhadap risiko keselamatan perlu dijalankan untuk menentukan keperluan integriti maklumat dan bagi mengenal pasti kaedah yang paling bersesuaian untuk dilaksanakan.	Pemilik Sistem ICT; Pentadbir Sistem
080204 Pengesahan Data *Output*	
Data yang dikeluarkan daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem
0803 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080301 Enkripsi	
Proses enkripsi (*encryption*) perlu dilaksanakan bagi melindungi kerahsiaan maklumat kritikal atau sensitif berdasarkan keperluan, dan penilaian risiko.	Semua

080302 Tandatangan Digital	
Penggunaan tandatangan digital kepada pengguna khususnya yang berurusan dengan transaksi maklumat kritikal atau sensitif atau maklumat rahsia rasmi secara elektronik.	Semua
080303 Pengurusan Kunci Kriptografi	
Pengurusan ke atas kunci kriptografi yang dilaksanakan ke atas maklumat kritikal atau sensitif hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
0804 Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080401 Kawalan Perisian (*Operational Software*)	
Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Proses pengemaskinian perisian hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan; b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan untuk digunakan; c) Mengaktifkan audit log bagi merekodkan aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; d) Mengawal capaian ke atas kod sumber bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;dan e) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal. f) Sistem konfigurasi perlu didokumenkan.	Pentadbir Sistem ICT
080402 Kawalan Data Pengujian Sistem	
Data pengujian sistem perlu dipilih dengan teliti, dilindungi dan	Pemilik Sistem

terkawal. Penggunaan data sebenar (*operational data*) yang melibatkan data personel atau data sensitif pada persekitaran pengujian adalah tertakluk kepada perjanjian *Non Disclosure Agreement* (NDA).	
080403 Kawalan Capaian kepada Kod Sumber (*Source Code*)	
Kawalan capaian kepada kod sumber perlu dilaksanakan bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. Kod sumber (*source code*) bagi aplikasi dan perisian adalah menjadi hak milik Datuk Bandar.	Pentadbir Sistem ICT
0805 Keselamatan Dalam Proses Pembangunan dan Penyelenggaraan	
Objektif: Menjaga dan menjamin keselamatan sistem perisian aplikasi dan maklumat.	
080501 Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dikawal, diuji, direkodkan dan disahkan melalui prosedur yang ditetapkan sebelum diguna pakai; b) Pengujian terhadap perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dilaksanakan dalam persekitaran yang berasingan samada daripada produksi atau pembangunan; c) 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; d) Mengawal perubahan dan /atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; e) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan f) Menghalang sebarang peluang untuk membocorkan dan	Pentadbir Sistem ICT, Pemilik Sistem.

memanipulasikan maklumat Datuk Bandar Kuala Lumpur.	
080502 Keperluan Kajian Teknikal Terhadap Aplikasi Selepas Perubahan Sistem Pengoperasian	
aplikasi perlu dikaji dan diuji apabila berlaku perubahan sistem pengoperasian bagi memastikan tiada sebarang kesan buruk yang merugikan kepada operasi dan keselamatan organisasi.	Pentadbir Sistem ICT
0806 Pengurusan Kelemahan Teknikal	
Objektif: Mengurangkan Risiko Akibat dari Eksploitasi Kelemahan Teknikal.	
080601 Kawalan Kelemahan Teknikal	
Kelemahan teknikal terhadap sistem maklumat perlu dilapor dan dibuat penilaian dengan segera untuk tindakan pembetulan. Perkara yang perlu dipatuhi adalah seperti berikut : a) Memperoleh maklumat teknikal yang tepat pada masanya ke atas system 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.	Pemilik Sistem; Pentadbir Sistem ICT

- BIDANG 09 -

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

BIDANG 09 - PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:
Memastikan insiden keselamatan ICT dan kelemahan dilapor dan disalur dengan cepat dan berkesan bagi meminimumkan proses pembaikan dan mengurangkan kesan insiden keselamatan ICT.

090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas asset ICT atau ancaman kemungkinan berlaku kejadian tersebut Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: a) Maklumat didapati hilang, atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	Personel, Pihak Ketiga

090102 Pelaporan Kelemahan Keselamatan

Pengguna sistem dikehendaki melaporkan sebarang kelemahan sistem dengan segera bagi mengelak insiden keselamatan ICT.	Personel

0902 Pengurusan Maklumat Insiden Keselamatan ICT

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

090201 Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan	CIO; ICTSO

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 DBKL. 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 : a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti bahan bukti; b) Menyalin bahan bukti dan merekodkan maklumat dan aktiviti penyalinan; c) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; dan e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	
090202 Pembelajaran Dari Insiden Kelemahan Maklumat	
Mewujudkan mekanisma bagi menentukan maklumat insiden keselamatan maklumat direkod untuk dianalisa dan dipantau.	Pentadbir Sistem ICT
090203 Pengumpulan Bukti	
Bukti-bukti insiden keselamatan maklumat perlu dikumpul dan dikekalkan untuk tindakan perundangan (jika perlu).	Pentadbir Sistem ICT

- BIDANG 10 -

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

BIDANG 10 - PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

Objektif:
Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

100101 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan - BCP*) 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 pihak pengurusan DBKL. Perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti 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; e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; f) Membuat *backup*; dan g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. BCP mempunyai empat komponen utama iaitu:- a) Pelan Pemulihan Bencana; b) Pelan Tindakbalas Kecemasan; c) Pelan Tindakbalas Insiden; dan d) Pelan Komunikasi.	CIO ICTSO; Pengurus ICT; Pentadbir Sistem ICT; Pemilik Sistem

dan hendaklah mengandungi perkara-perkara berikut:

a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b) Senarai personel DBKL dan vendor berserta 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 di mana boleh.

Salinan BCP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP 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 dibangunkan.

Ujian BCP hendaklah dijadualkan untuk memastikan ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. Salinan BCP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

- BIDANG 11 -

PEMATUHAN

BIDANG 11 - PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

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

110101 Pematuhan Dasar

Personel dan pihak ketiga hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT DBKL dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Aset ICT di DBKL termasuk maklumat yang disimpan di dalamnya adalah hak milik Datuk Bandar. Datuk Bandar berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT DBKL selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber DBKL.	Semua

110102 Pematuhan dengan Dasar dan Keperluan Teknikal

ICTSO hendaklah memastikan prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar dan keperluan teknikal.	ICTSO

110103 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

110104 Keperluan Perundangan	
Pengguna aset ICT DBKL perlu mematuhi segala keperluan perundangan, akta atau peraturan-peraturan lain yang berkaitan.	Semua
110105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT DBKL boleh dikenakan tindakan tatatertib di bawah Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000.	Semua

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
De-Militarised Zone (DMZ)	*De-Militarised Zone(DMZ)* merupakan zon yang membenarkan capaian daripada internet dan dikawal melalui firewall.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada *port* yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.

GLOSARI	
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
VLAN	*Virtua Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
VPN	*Virtual Private Network*
NTP	*Network Time Protocol*
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Off-the-shelves	Peralatan yang dihasilkan secara komersial, *ready made, standardized*, dan *regularly available equipment*, barangan, alat ganti, perisian, dan sebagainya.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
MODEM	MOdulator DEModulator

GLOSARI	
	Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

BRG/JPM/18/02

BORANG AKUAN PEMATUHAN
DASAR KESELAMATAN ICT DBKL

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan/Bahagian : .....

Adalah saya dengan ini mengaku bahawa :-

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

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....

(Nama Pegawai Keselamatan ICT)

b.p. Datuk Bandar Kuala Lumpur

Tarikh: .....

Lampiran 2

SENARAI PERUNDANGAN DAN PERATURAN

1. Peraturan-peraturan DBKL (Kewangan dan Perakaunan) 2007
2. Peraturan-Peraturan DBKL (Pelantikan, Kenaikan Pangkat Dan Penamatan Perkhidmatan) 2009
3. Peraturan-Peraturan Kewangan DBKL 2007 (Pindaan 2009)
4. Pekeliling HRMIS - Data Perjawatan Bil.12 Tahun 2005
5. Garis Panduan Keselamatan DBKL
6. Garis Panduan Garis Panduan Pengurusan Rekod dan Fail DBKL
7. Akta Tandatangan Digital 1997
8. Akta Rahsia Rasmi 1972
9. Akta Jenayah Komputer 1997
10. Akta Hak Cipta (Pindaan) Tahun 1997
11. Akta Komunikasi dan Multimedia 1998
12. Arahan Teknologi Maklumat 2007
13. Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000