DASAR KESELAMATAN ICT

MAJLIS PERBANDARAN KOTA BHARU
BANDAR RAYA ISLAM

VERSI 1.0

JAN 2012

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT MPKB-BRI	Versi 1.0	01/ 01 / 2012	1 dari 48

KANDUNGAN **MUKA SURAT**

TAFSIRAN 5

PENDAHULUAN

I. Pengenalan 7
II. Objektif 7
III. Skop 7
IV. Prinsip-Prinsip 7

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

Dasar Keselamatan ICT 10
1.1 Pelaksanaan Dasar 10
1.2 Penyebaran Dasar 10
1.3 Penyelenggaraan Dasar 10
1.4 Pengecualian Dasar 10

PERKARA 02 ORGANISASI KESELAMATAN

Struktur Organisasi Keselamatan 11
2.1 Yang Dipertua, Setiausaha MPKB-BRI 11
2.2 Jawatankuasa Penyelaras Keselamatan ICT 11
2.2.1 Setiausaha (CIO) 11
2.2.2 Pegawai Keselamatan ICT (ICTSO) 12
2.2.3 Pengurus Komputer 13
2.2.4 Pentadbir Sistem ICT 13
2.2.5 Penyelaras ICT 14
2.3 Pengguna 15
2.4 Pihak Ketiga 16

PERKARA 03 KAWALAN DAN PENGELASAN ASET

Akauntabiliti Aset 17
3.1 Inventori Aset 17
3.2 Pengkelasan Maklumat 17
3.3 Pengendalian Maklumat 18

PERKARA 04 KESELAMATAN SUMBER MANUSIA

Keselamatan Sumber Manusia 19
4.1 Sebelum Berkhidmat 19
4.2 Dalam Perkhidmatan 19
4.3 Bertukar atau Tamat Perkhidmatan 20

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Keselamatan Kawasan 21
5.1 Perimeter Keselamatan Fizikal 21
5.2 Kawalan Masuk Fizikal 21
Keselamatan Aset ICT 22
5.3 Perkakasan 22
5.4 Dokumen 22
5.5 Media Storan 23
Keselamatan Persekitaran 24
5.6 Kawalan Persekitaran 24
5.7 Bekalan Kuasa 25
5.8 Prosedur Kecemasan 25
5.9 Keselamatan Kabel 25
5.10 Penyelenggaraan Peralatan ICT 26
5.11 Peminjaman Peralatan Untuk Kegunaan Di Luar Pejabat 26
5.12 Pengendalian Peralatan Luar Yang Dibawa Masuk 27
5.13 Pelupusan dan Kitar Semula Peralatan 27
5.14 *Clear Desk* dan *Clear Screen* 27

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

Pengurusan Prosedur Operasi 28
6.1 Pengendalian Prosedur 28
6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga 28
6.3 Perancangan dan Penerimaan Sistem 29
6.4 Perlindungan dari Kod Jahat 30
6.5 *Housekeeping* 31
6.5.1 Penduaan 31
6.5.2 Sistem Log 31
Pengurusan Rangkaian 32
6.6 Kawalan Infrastruktur Rangkaian 32
Pengurusan Media 34
6.7 Penghantaran dan Pemindahan 34
6.8 Pengendalian Media 34
Keselamatan Komunikasi 35
6.9 Internet 35
6.10 Mel Elektronik 35

PERKARA 07 PENGURUSAN INSIDEN KESELAMATAN ICT

Menangani Insiden Keselamatan ICT 36
7.1 Prosedur Pengurusan Insiden 36
7.2 Pelaporan Insiden 36

PERKARA 08 KAWALAN CAPAIAN

Kawalan Capaian 37
8.1 Keperluan Dasar 37
8.2 Pengurusan Capaian Pengguna 37
8.3 Tanggungjawab Pengguna 38
8.4 Kawalan Capaian Rangkaian 38
8.5 Kawalan Capaian Sistem Operasi 39
8.6 Kawalan Capaian Aplikasi dan Maklumat 40
8.7 Penggunaan Peralatan ICT Mudah Alih 40

PERKARA 09 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Perolehan, Pembangunan dan Penyelenggaraan Sistem dan Aplikasi 41
9.1 Keperluan Keselamatan 41
9.2 Kawalan Kriptografi 41
9.3 Kawalan Perisian Operasi 42
9.4 Keselamatan Dalam Proses Pembangunan dan Sokongan 42

PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Dasar Kesinambungan Perkhidmatan 43
10.1 Pelan Kesinambungan Perkhidmatan 43

PERKARA 11 PEMATUHAN

Pematuhan dan Keperluan Perundangan 44
11.1 Pematuhan Dasar 44
11.2 Keperluan Perundangan 44

TAFSIRAN

Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia, hendaklah diperingkatkan Rahsia Besar.
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing hendaklah diperingkatkan Rahsia.
Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing hendaklah diperingkatkan Sulit.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakan juga diberi satu tahap perlindungan keselamatan hendaklah diperingkatkan Terhad.
Ketua Jabatan / Bahagian	Yang Dipertua, Ahli Majlis, Setiausaha, Pengarah, Ketua Penolong Pengarah dan Penolong Pengarah.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (*soft copy*), elektronik, dalam talian, kertas lutsinar, risalah atau slaid.
Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, kartrij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab MPKB-BRI

TAFSIRAN

Akaun pengguna	akaun e mel dan rangkaian
Kawasan Terperingkat	Kawasan-kawasan premis atau sebahagian dari premis di mana perkara-perkara terperingkat disimpan atau diuruskan atau di mana kerja terperingkat dijalankan.
Pihak Ketiga	Pihak yang membekalkan perkhidmatan kepada MPKB-BRI
Peralatan perlindungan	Peralatan yang berfungsi untuk pengawalan, pencegahan dan pengurusan tampalan seperti firewall, router, proxy, antivirus, dll
Insiden Keselamatan	Bermaksud musibah (*adverse event*) yang berlaku ke atas sistem maklumat
Enkripsi	Bermaksud menjadikan teks biasa (*plaintext*) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks *cipher .* Bagi mendapatkan semula teks biasa tersebut, penyahsulitan digunakan.
Kriptografi	Bermaksud adalah satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.
Pengguna	Kakitangan MPKB-BRI, pembekal, pakar runding, dll
Warga MPKB-BRI	Kakitangan MPKB-BRI

PENDAHULUAN

I. Pengenalan

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang perlu dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Majlis Perbandaran Kota Bharu Bandar Raya Islam (MPKB-BRI). Dasar ini juga menerangkan kepada semua pengguna di MPKB-BRI mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MPKB-BRI.

II. Objektif

Dasar Keselamatan ICT MPKB-BRI diwujudkan untuk memastikan tahap keselamatan ICT MPKB-BRI terurus dan dilindungi bagi menjamin kesinambungan urusan MPKB-BRI dengan meminimumkan kesan insiden keselamatan ICT.

III. Skop

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

a. Maklumat (contoh: fail, dokumen, data elektronik),
b. Perisian (contoh: aplikasi dan sistem perisian) dan
c. Fizikal (contoh: komputer, peralatan komunikasi dan media magnet).

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

IV. Prinsip-Prinsip

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

a. Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

PENDAHULUAN

b. Hak Akses Minimum

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

c. Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT MPKB-BRI;

d. Pengasingan

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

e. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan(*server*), *router, firewall, IPS, Antivirus* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

f. Pematuhan

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

PENDAHULUAN

g. Pemulihan

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

h. Saling Bergantungan

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

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

Dasar Keselamatan ICT	
1.1 Pelaksanaan Dasar	**Tanggungjawab**
Yang Dipertua MPKB-BRI adalah bertanggungjawab ke atas pelaksanaan arahan dengan dibantu oleh Jawatankuasa Penyelaras Keselamatan ICT yang terdiri daripada Setiausaha (CIO), Pengurus Komputer, Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.	Yang Dipetua, Setiausaha atau Pegawai yang diturunkan kuasa
1.2 Penyebaran Dasar	
Dasar ini bertujuan memastikan hala tuju pengurusan keselamatan kementerian untuk melindungi asset ICT selaras dengan keperluan perundangan. Dasar ini perlu disebarkan kepada semua pengguna MPKB-BRI (termasuk kakitangan, pembekal, pakar runding dan lain-lain yang berurusan dengan MPKB-BRI)	ICTSO
1.3 Penyelenggaraan Dasar	
Dasar Keselamatan ICT MPKB-BRI adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan organisasi. Prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT MPKB-BRI adalah seperti berikut: a. Mengkaji semula dasar ini sekurang-kurangnya sekali setahun bag mengenal pasti dan menentukan perubahan yang diperlukan; b. Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Jawatankuasa Pemandu ICT (JPICT) Kementerian; c. Memaklumkan perubahan yang telah dipersetujui oleh JPICT kepada semua pengguna.	ICTSO
1.4 Pemakaian Dasar	
Dasar Keselamatan ICT MPKB-BRI adalah terpakai kepada semua pengguna ICT MPKB-BRI dan tiada pengecualian diberikan.	Semua Pengguna MPKB-BRI

PERKARA 02 ORGANISASI KESELAMATAN

Struktur Organisasi Keselamatan	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.	
2.1 Yang Dipertua MPKB-BRI	**Tanggungjawab**
Peranan dan tanggungjawab Yang Dipertua adalah seperti berikut: a. Memastikan pelaksanaan Jawatankuasa Penyelaras Keselamatan ICT MPKB-BRI; b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MPKB-BRI; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MPKB-BRI.	Yang Dipertua atau Pegawai yang diturunkan kuasa
2.2 Jawatankuasa Penyelaras Keselamatan ICT	
Objektif : Menerangkan peranan dan tanggungjawab ahli pasukan penyelaras keselamatan MPKB-BRI	
2.2.1 Setiausaha MPKB-BRI (CIO)	
Peranan dan tanggung jawab CIO adalah seperti berikut: a. Mewujud dan mengetuai pasukan penyelaras keselamatan ICT MPKB-BRI; b. Menasihati ketua Setiausaha MPKB-BRI dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; c. Menentukan keperluan keselamatan ICT; d. Menyelaras pembangunan dan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan e. Memastikan semua pengguna memahami peruntukan di bawah Dasar Keselamatan ICT MPKB-BRI.	CIO

PERKARA 02 ORGANISASI KESELAMATAN

2.2.2 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO adalah seperti berikut: a. Mengurus program-program keselamatan ICT; b. Menguatkuasa dan memantau pematuhan ke atas Dasar Keselamatan ICT ; c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT kepada semua pengguna; d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT; e. Menjalankan pengurusan risiko; f. Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan MPKB-BRI berdasarkan hasil penemuan/keperluan semasa dan menyediakan laporan mengenainya; g. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO; i. Mengenal pasti punca ancaman atau insiden keselamatan ICT dan melaksanakan langkah-langkah baik pulih dengan segera; j. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT MPKB-BRI; dan k. Membangun, menyelaras dan melaksana pelan latihan dan program kesedaran keselamatan ICT.	ICTSO

PERKARA 02 ORGANISASI KESELAMATAN

2.2.3 Pengurus Komputer	**Tanggungjawab**
Peranan dan tanggungjawab Pengurus Komputer adalah seperti berikut: a. Memahami dan mematuhi Dasar Keselamatan ICT MPKB-BRI; b. Menentukan kawalan akses semua pengguna terhadap aset ICT MPKB-BRI; c. Melaporkan sebarang perkara atau ancaman ke atas keselamatan ICT kepada ICTSO; dan d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPKB-BRI.	Ketua Unit ICT / Pegawai yang diturunkan kuasa
2.2.4 Pentadbir Sistem ICT	
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MPKB-BRI; c. Memastikan kerahsiaan kata laluan dan memantau aktiviti capaian harian pengguna; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. Menyimpan dan menganalisis rekod jejak audit (*audit trail*); dan f. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	Pentadbir Sistem ICT

PERKARA 02 ORGANISASI KESELAMATAN

2.2.5 Penyelaras ICT Jabatan/ Bahagian Peranan dan tanggungjawab Penyelaras ICT adalah seperti berikut:	
a. Melaksanakan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPKB-BRI; b. Menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta melaksanakan langkah-langkah perlindungan yang bersesuaian; c. Melaporkan insiden keselamatan ICT kepada ICTSO. d. Mengenal pasti punca ancaman atau insiden keselamatan ICT dan melaksanakan langkah-langkah baik pulih dengan segera; e. Melaporkan sebarang salahlaku pengguna yang melanggar Dasar Keselamatan ICT MPKB-BRI kepada CTSO;dan f. Melaksanakan program-program kesedaran mengenai keselamatan ICT.	Penyelaras ICT

PERKARA 02 ORGANISASI KESELAMATAN

2.3 Pengguna ICT MPKB-BRI	Tanggungjawab
Pengguna adalah termasuk kakitangan MPKB-BRI, pembekal, pakar runding dll. Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Memahami dan mematuhi Dasar Keselamatan ICT MPKB-BRI; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melepasi tapisan keselamatan (jika berkaitan); d. Mematuhi prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat MPKB-BRI; e. Mengambil langkah-langkah perlindungan seperti berikut :- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan 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. f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Penyelaras ICT dengan segera; dan g. Menyertai program-program kesedaran mengenai keselamatan ICT.	Semua Pengguna MPKB-BRI

PERKARA 02 ORGANISASI KESELAMATAN

2.4 Pihak Ketiga/luar	
Keselamatan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga/ luar hendaklah sentiasa dikawal. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: a. Dasar Keselamatan ICT MPKB-BRI; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; d. Hak Harta Intelek; Nota 1: Surat Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk “Tatacara Pengurusan Perolehan Kerajaan Secara Tender” dan Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk “Peraturan Perolehan Perkhidmatan Perundingan” yang berkaitan juga boleh dirujuk.	Penyelaras ICT Jabatan/Bahagian, Pentadbir Sistem ICT

PERKARA 03 KAWALAN DAN PENGELASAN ASET

Akauntabiliti Aset	
Objektif : Memberi dan menyokong perlindungan yang optimum ke atas semua aset ICT MPKB-BRI.	
3.1 Inventori Aset	**Tanggungjawab**
Memastikan semua aset ICT MPKB-BRI hendaklah diberi perlindungan yang bersesuaian oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset dikenal pasti dan maklumat aset direkodkan dalam daftar daftar harta modal dan inventori (TPA Kew 2) dan sentiasa kemaskini. b. Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan c. Mengenal pasti, mendokumen dan melaksanakan peraturan bagi penggunaan aset.	Semua pengguna MPKB-BRI
3.2 Pengkelasan Maklumat Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan kepada tahap sensitiviti masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a. Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal MPKB-BRI. Setiap maklumat hendaklah dikelas dan dilabelkan mengikut sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: i. Rahsia Besar; ii. Rahsia; iii. Sulit; atau iv. Terhad.	Pegawai yang diberi tanggungjawab

PERKARA 03 KAWALAN DAN PENGELASAN ASET

<table>
<tr><td>3.3 Pengendalian Maklumat</td><td></td></tr>
<tr><td>Pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penyalinan, penghantaran, penyampaian, penukaran dan pemusnahan 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 dan garis panduan keselamatan yang ditetapkan;

f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penyalinan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

g. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.</td><td>Semua Pengguna MPKB-BRI</td></tr>
</table>

PERKARA 04 KESELAMATAN SUMBER MANUSIA

Keselamatan Sumber Manusia	
Objektif: Untuk memastikan semua sumber manusia yang terlibat termasuk penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat memahami tanggungjawab dan peranan mereka dalam keselamatan aset ICT.	
4.1 Sebelum Berkhidmat	**Tanggungjawab**
Memastikan penjawat awam, kontraktor, pihak ketiga, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Menjalankan tapisan keselamatan untuk penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan; dan b. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Semua Pengguna MPKB-BRI
4.2 Dalam Perkhidmatan	
Memastikan semua pengguna sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong dasar keselamatan ICT MPKB-BRI. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua pengguna MPKB-BRI mengurus keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh MPKB-BRI; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan ICT diberi kepada semua pengguna MPKB-BRI dan sekiranya perlu kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; dan c. Memastikan adanya proses tindakan disiplin ke atas semua pengguna MPKB-BRI sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan oleh MPKB-BRI.	Semua Pengguna MPKB-BRI

PERKARA 04 KESELAMATAN SUMBER MANUSIA

4.3 Bertukar Atau Tamat Perkhidmatan	
Memastikan semua pengguna MPKB-BRI yang tamat perkhidmatan atau bertukar dari MPKB-BRI diurus dengan teratur. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT Kerajaan dikembalikan kepada MPKB-BRI mengikut peraturan dan/atau terma yang ditetapkan oleh MPKB-BRI; dan b. Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MPKB-BRI.	Semua pengguna MPKB-BRI

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Keselamatan Kawasan	
Objektif : Mencegah akses fizikal yang tidak dibenarkan, yang boleh mengakibatkan kecurian, kerosakan dan gangguan kepada premis dan maklumat.	
5.1 Perimeter Keselamatan Fizikal	**Tanggungjawab**
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mengenalpasti kawasan keselamatan fizikal dengan jelas dan lokasi serta keteguhan kawasan hendaklah bergantung kepada keperluan untuk melindungi aset dalam kawasan tersebut dan hasil dari penilaian risiko; b. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memperkukuhkan dinding dan siling; d. Memasang alat penggera atau kamera litar tertutup (CCTV), jika berkaitan; e. Menghadkan laluan keluar masuk; f. Mengadakan kaunter kawalan; g. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan h. Mewujudkan perkhidmatan kawalan keselamatan.	CIO, ICTSO dan Penyelaras ICT
5.2 Kawalan Masuk Fizikal	
Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis/ bangunan MPKB-BRI. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mempamerkan pas keselamatan sepanjang waktu bertugas; dan b. Mendaftar dan mendapat Pas Keselamatan Pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan bagi setiap pelawat/ pihak luar.	Semua Pengguna MPKB-BRI

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Keselamatan Aset ICT	
Objektif: Melindungi peralatan dan maklumat daripada kehilangan, kerosakan, kecurian atau salah guna yang mendatangkan gangguan ke atas aktiviti MPKB-BRI.	
5.3 Perkakasan	**Tanggungjawab**
Peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh berfungsi apabila diperlukan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memeriksa dan memastikan semua perkakasan ICT di bawah kawalan setiap pengguna berfungsi dengan sempurna; b. Menyimpan atau meletakkan semua perkakasan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; c. Menjadi tanggungjawab setiap pengguna di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan d. Melaporkan sebarang bentuk penyelewengan atau salah guna perkakasan kepada ICTSO / Penyelaras ICT di MPKB-BRI.	Semua Pengguna MPKB-BRI
5.4 Dokumen	
Langkah-langkah pengurusan dokumen yang baik dan selamat perlu dilaksanakan bagi memastikan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; c. Menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan d. Memastikan dokumen yang mengandungi bahan atau maklumat terperingkat diambil segera dari media output.	Semua Pengguna MPKB-BRI

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.5 Media Storan	
Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat. Perkara yang perlu dipatuhi adalah seperti berikut: a. Menyediakan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Menghadkan akses untuk memasuki kawasan penyimpanan media kepada pengguna yang dibenarkan sahaja; c. Merujuk kepada tatacara pelupusan sekiranya penghapusan maklumat hendak dilakukan dan mestilah mendapat kebenaran pemilik maklumat terlebih dahulu; dan d. Merekodkan pengurusan media termasuk inventori, pergerakan dan penduaan (*backup*).	Semua Pengguna MPKB-BRI

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Keselamatan Persekitaran	
Objektif: Melindungi aset ICT MPKB-BRI dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
5.6 Kawalan Persekitaran	**Tanggungjawab**
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Perkara yang perlu dipatuhi adalah seperti berikut: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Memasang peralatan perlindungan hendaklah di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Menyimpan bahan mudah terbakar hendaklah di luar kawasan kemudahan penyimpanan aset ICT; e. Meletakkan semua bahan cecair hendaklah di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Melarang pengguna merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT; dan g. Memeriksa dan menguji semua peralatan perlindungan sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	Semua Pengguna MPKB-BRI

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.7 Bekalan Kuasa	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan peralatan sokongan seperti UPS (Uninterruptable Power *Supply)* dan penjana *(generator)* bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; b. Memeriksa dan menguji semua peralatan sokongan bekalan kuasa secara berjadual; dan c. Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai.	Pengarah,Ketua Penolong Pengarah dan Penolong Pengarah
5.8 Prosedur Kecemasan	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada prosedur kecemasan yang telah ditetapkan; b. Melaporkan insiden kecemasan persekitaran dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ); c. Mengada, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa; dan d. Merancang dan mengadakan latihan kebakaran bangunan (*fire drill*) secara berkala.	Semua Pengguna MPKB-BRI
5.9 Keselamatan Kabel	
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kabel mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan wire tapping; dan d. Melabelkan kabel menggunakan kod standard.	

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.10 Penyelenggaraan Peralatan ICT	
Peralatan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggarakan; b. Memastikan perkakasan hanya diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Memeriksa dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan d. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Penyelaras ICT
5.11 Peminjaman Peralatan Untuk Kegunaan Di Luar Pejabat	
Peralatan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mendapatkan kelulusan mengikut peraturan dibawah Pekeliling Perbendaharaan Tatacara Pengurusan Aset atau peraturan MPKB-BRI bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; b. Melindungi dan mengawal peralatan sepanjang masa; c. Memastikan aktiviti peminjaman dan pemulangan peralatan ICT direkodkan; dan d. Menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap.	Pengarah,Ketua Penolong Pengarah dan Penolong Pengarah

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.12 Pengendalian Peralatan Luar Yang Dibawa Masuk	
Bagi peralatan yang dibawa masuk ke premis kerajaan, perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT MPKB-BRI; b. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh MPKB-BRI bagi membawa masuk/ keluar peralatan; dan c. Memriksa dan memastikan peralatan ICT yang dibawa keluar tidak mengandungi meklumat kerajaan. Ia perlu disalin dan dihapuskan.	Penyelaras ICT
5.13 Pelupusan Dan Kitar Semula Peralatan	
Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPKB-BRI: a. Menghapuskan semua kandungan khususnya maklumat rahsia rasmi terlebih dahulu sama ada melalui *shredding*, *grinding, degauzing* atau pembakaran sebelum pelupusan; dan b. Merujuk kepada Pekeliling Perbendaharaan Bil. 5 Tahun 2007 “Tatacara Pengurusan Aset Alih Kerajaan.	Semua Pengguna MPKB-BRI
5.14 *Clear Desk* Dan *Clear Screen*	
Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b. Menyimpan bahan-bahan sensitif di dalam laci atau cabinet fail yang berkunci; dan c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Semua pengguna MPKB-BRI

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

Pengurusan Prosedur Operasi	
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.	
6.1 Pengendalian Prosedur	**Tanggungjawab**
Memastikan kemudahan pemprosesan maklumat beroperasi seperti yang ditetapkan dan selamat. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mendokumenkan semua prosedur keselamatan ICT yang di wujud, dikenal pasti dan masih diguna pakai, disimpan dan dikawal; b. Memastikan setiap prosedur mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Mengemaskini semua prosedur hendaklah dari semasa ke semasa atau mengikut keperluan.	ICTSO dan Penyelaras ICT
6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Memantau, menyemak semula dan mengaudit perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga dari semasa ke semasa; dan c. Mengurus perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambahbaik polisi keselamatan, prosedur dan kawalan maklumat sedia ada dengan mengambilkira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Pentadbir Sistem ICT

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

6.3 Perancangan Dan Penerimaan Sistem	
Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem. Perkara yang perlu dipatuhi adalah seperti berikut: a. Merancang, mengurus dan mengawal kapasiti sesuatu komponen atau sistem ICT dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; b. Memantau, menala dan merancang penggunaan peralatan bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem di tahap optimum; c. Menetap kriteria penerimaan untuk sistem maklumat baru, peningkatan dan versi baru dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem; dan d. Mengambil kira ciri-ciri keselamatan ICT dalam perancangan keperluan kapasiti bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

6.4 Perlindungan Dari Kod Jahat (*Malicious Code*)	
Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *worm, trojan dan spyware*. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan *Intrusion Detection System (IDS)* dan mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang berlesen dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini *pattern* anti virus dari semasa ke semasa; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri program kesedaran secara berkala mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT dari semasa ke semasa.	Semua Pengguna MPKB-BRI

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

6.5 *Housekeeping*	
Mengekalkan integriti, kebolehsediaan maklumat dan kemudahan pemprosesan maklumat.	
6.5.1 Penduaan (*Backup*)	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan hendaklah direkodkan dan disimpan di lokasi yang berlainan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut kesesuaian operasi; c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan d. Membuat dan menguji salinan maklumat dan perisian secara berkala berdasarkan prosedur penduaan.	Pentadbir Sistem ICT
6.5.2 Sistem Log	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan.	Pentadbir Sistem ICT

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

Pengurusan Rangkaian

Objektif: Memastikan perlindungan keselamatan maklumat dalam rangkaian dan infrastruktur sokongan terurus dan terkawal.

6.6 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara yang perlu dipatuhi adalah seperti berikut: a. Membangun dan melaksanakan polisi dan prosedur bagi melindungi maklumat berhubung kait dengan sistem rangkaian; b. Mengenalpasti ciri-ciri keselamatan, tahap perkhidmatan rangkaian dan memasukkannya kedalam mana-mana perjanjian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar; c. Mengasingkan tanggungjawab atau kerja-kerja operasi rangkaian dan komputer untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; d. Meletakkan peralatan rangkaian hendaklah di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan selamat; e. Mengawal capaian kepada peralatan rangkaian dan terhad kepada pengguna yang dibenarkan sahaja; f. Memastikan semua peralatan melalui proses *Factory Acceptance Check (FAC)* semasa pemasangan dan konfigurasi; g. Memastikan semua trafik rangkaian melalui firewall di bawah kawalan MPKB-BRI; h. Melarang semua perisian sniffer atau network analyser dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; i. Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MPKB-BRI;	Pentadbir Sistem ICT

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

j. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan"; k. Mendapat kebenaran ICTSO bagi sebarang penyambungan rangkaian yang bukan di bawah kawalan MPKB-BRI; l. Memastikan penggunaan LAN tanpa wayar di MPKB-BRI mematuhi MAMPU surat UPTM (S) 159/338/8 Jilid 30 (84) bertajuk "Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar W (Wireless LAN) di Agensi-agensi Kerajaan.	

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

Pengurusan Media	
Objektif: Melindungi media ICT dari kerosakan dan penyalahgunaan	
6.7 Penghantaran Dan Pemindahan	**Tanggungjawab**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan dan tertakluk kepada prosedur yang sedia ada.	Pentadbir Sistem ICT
6.8 Pengendalian Media	
Prosedur bertujuan mengendali dan menyimpan maklumat daripada didedah tanpa kebenaran atau disalah guna. Perkara yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Menghadkan pengedaran media untuk tujuan yang dibenarkan; d. Merekod dan mengawal aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Menghapus atau memusnahkan media yang mengandungi maklumat rahsia rasmi hendaklah mengikut prosedur keselamatan media yang dikeluarkan oleh kerajaan.	Pentadbir Sistem ICT

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

Keselamatan Komunikasi Rangkaian	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian dalam MPKB-BRI dan mana-mana agensi luar terjamin.	
6.9 Internet	**Tanggungjawab**
Penggunaan internet hendaklah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan pekeliling–pekeliling yang dikeluarkan oleh kerajaan dari semasa ke semasa.	Semua Pengguna MPKB-BRI
6.10 Mel Elektronik	
Penggunaan mel elektronik hendaklah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan pekeliling yang dikeluarkan oleh pihak kerajaan dari semasa-semasa	Semua Pengguna MPKB-BRI

PERKARA 07 PENGURUSAN INSIDEN KESELAMATAN ICT

Menangani Insiden Keselamatan ICT	
Objektif: Memastikan tindakan menangani insiden keelamatan ICT diambil dengan cepat, teratur dan berkesan serta meminimumkan kesan insiden keselamatan ICT.	
7.1 Prosedur Pengurusan Insiden	**Tanggungjawab**
Prosedur pengurusan insiden perlu diwujudkan dan didokumenkan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mengenalpasti semua jenis insiden keselamatan ICT sperti gangguan perkhidmatan yang disengajakan, pemalsuan *identity* dan pengubahsuaan perisian tanpa kebenaran; b. Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. Menyimpan audit trail dan memelihara bahan bukti; dan d. Menyediakan pelan tindakan pemulihan segera.	ICTSO
7.2 Pelaporan Insiden	
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO / Penyelaras Keselamatan ICT Jabatan/Bahagian dengan kadar segera. Insiden keselamatan ICT adalah termasuk yang berikut: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Nota 2: Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan ICT” mengenainya bolehlah dirujuk.	Semua Pengguna MPKB-BRI

PERKARA 08 KAWALAN CAPAIAN

<table>
<tr><th colspan="2">Kawalan Capaian</th></tr>
<tr><td colspan="2">Objektif : Memahami dan mematuhi keperluan keselamatan dalam membuat capaian dan menggunakan aset ICT MPKB-BRI.</td></tr>
<tr><td>8.1 Keperluan Dasar</td><td>Tanggungjawab</td></tr>
<tr><td>Capaian kepada aset ICT hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan dipantau dan menyokong dasar kawalan capaian pengguna sedia ada.</td><td>Semua Pengguna MPKB-BRI</td></tr>
<tr><td>8.2 Pengurusan Capaian Pengguna</td><td></td></tr>
<tr><td>Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.

Perkara yang perlu dipatuhi adalah seperti berikut:

a. Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk membuat capaian maklumat dan perkhidmatan;

b. Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat;

c. Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran Ketua Jabatan secara bertulis dan direkodkan;

d. Pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan Jabatan dan tindakan pengemaskinian dan/atau pembatalan hendaklah diambil atas sebab berikut:

i. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Ketua Jabatan;

ii. Pengguna bercuti atau bertugas di luar pejabat dalam satu tempoh yang lama seperti mana yang ditetapkan oleh Ketua Jabatan;

iii. Pengguna bertukar jawatan, tanggungjawab dan/atau dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib; dan

iv. Pengguna bertukar, berpindah, bersara dan/atau tamat perkhidmatan.

e. Merekod dan menyenggara aktiviti capaian oleh pengguna dengan sistematik dan dikaji dari semasa ke semasa. Maklumat yang direkod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.</td><td>Pentadbir Sistem atau Penyelaras ICT</td></tr>
</table>

PERKARA 08 KAWALAN CAPAIAN

8.3 Tanggungjawab Pengguna	
Memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan; b. Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan c. Mematuhi amalan *clear desk/ clear screen policy.*	Semua Pengguna MPKB-BRI
8.4 Kawalan Capaian Rangkaian	
Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan menempatkan atau memasang antaramuka diantara rangkaian MPKB-BRI dan lain-lain cawangan serta mewujud dan menguatkuasa mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan pengguna boleh membuat capaian ke atas perkhidmatan yang dibenarkan sahaja; b. Mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh; c. Mengguna kaedah pengenalan automatik berdasarkan lokasi dan peralatan untuk pengesahan sambungan ke dalam rangkaian; d. Mengawal capaian fizikal dan logikal keatas kemudahan port diagnostic dan konfigurasi jarak jauh; e. Mengasingkan capaian mengikut kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat dalam rangkaian; f. Mengawal sambungan ke rangkaian, khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan MPKB-BRI; dan g. Mewujud dan melaksana kawalan pengalihan laluan (routing control) untuk memastikan pematuhan ke atas peraturan MPKB-BRI.	

PERKARA 08 KAWALAN CAPAIAN

8.5 Kawalan Capaian Sistem Operasi	
Memastikan capaian ke atas sistem operasi dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong perkara berikut: a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan MPKB-BRI; b. Mewujudkan *audit trail* ke atas semua capaian sistem operasi terutama pengguna bertaraf khas (*super user*); c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; d. Menyedia kaedah sesuai untuk pengesahan capaian (authentication); dan e. Menghadkan tempoh penggunaan mengikut kesesuaian. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal capaian ke atas sistem operasi menggunakan prosedur *log-on* yang selamat; b. Prosedur lo-gon yang selamat perlulah: ii. Menggunakan kaedah pengenalan pengguna yang unik dan teknik pengesahan pengguna yang berkesan dan selamat; iii. Melaksana sisten pengurusan kata laluan yang interaktif dan menjamin kualiti serta keselamatan kata laluan; iv. Mengawal penggunaan utiliti yang berkeupayaan melepasi sistem dan aplikasi terhad; v. Menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan; dan vi. Menghadkan tempoh masa penggunaan bagi meningkatkan keselamatan aplikasi yang berisiko tinggi.	

PERKARA 08 KAWALAN CAPAIAN

8.6 Kawalan Capaian Aplikasi Dan Maklumat	
Capaian sistem dan aplikasi di MPKB-BRI adalah terhad kepada pengguna dan tujuan yang dibenarkan sahaja. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: a. Membenarkan pengguna membuat capaian aplikasi dan maklumat yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat daripada utiliti yang sedia ada dalam sistem operasi dan perisian malicious yang berupaya melangkaui kawalan sistem. Perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna perlu dihadkan, selaras dengan peraturan MPKB-BRI; dan b. Mengasingkan persekitaran pengkomputeran yang khusus bagi sistem yang sensitif.	Pentadbir Sistem ICT
8.7 Penggunaan Peralatan ICT Mudah Alih	
Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan ICT mudah alih. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; dan b. Mewujudkan peraturan dan garis panduan untuk memastikan persekitaran kerja jarak jaun adalah sesuai dan selamat.	Pentadbir Sistem ICT

PERKARA 09 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Perolehan, Pembangunan Dan Penyelenggaraan Sistem Dan Aplikasi	
Objektif : Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
9.1 Keperluan Keselamatan	**Tanggungjawab**
Memastikan kawalan keselamatan yang sesuai dijalinkan ke dalam aplikasi bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahguaan maklumat dalam aplikasi. Perkara yang perlu dipatuhi adalah seperti berikut: a. Menyemak dan mengesahkan data sebelum dimasukkan ke dalam aplikasi bagi menjamin ketepatan maklumat; b. Menggabungkan semakan pengesahan di dalam aplikasi untuk mengenalpasti sebarang pencemaran maklumat sama ada kerana kesilapan atau disengajakan; c. Mengenalpasti dan melaksana kawalan yang sesuai bagi pengesahan dan perlindungan integriti mesej dalam aplikasi; dan d. Menjalankan proses semak ke atas hasil data daripada setiap proses aplikasi untuk menjamin ketepatan dan kesesuaian.	Pemilik sistem, Pentadbir Sistem ICT, ICTSO
9.2 Kawalan Kriptografi	
Memastikan kaedah kriptografi diguna untuk melindungi kerahsiaan, kesahihan dan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: a. Membangun dan melaksana peraturan untuk melindungi maklumat menggunakan kaedah kriptografi yang sesuai; dan b. Memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi diguna pakai di MPKB-BRI.	Pentadbir Sistem ICT

PERKARA 09 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

9.4 Kawalan Perisian Operasi	
Memastikan kaedah yang sesuai dilaksanakan untuk mengawal capaian ke atas fail system dan kod sumber program bagi menjamin keselamatan sistem fail. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mewujudkan peraturan untuk mengawal pemasangan perisian ke dalam persekitaran operasi; b. Mewujudkan peraturan untuk pemilihan, perlindungan dan kawalan data ujian; dan c. Mengawal dan menghadkan capaian ke atas kod sumber kepada pengguna yang dibenarkan sahaja.	Pentadbir Sistem ICT
9.5 Keselamatan Dalam Proses Pembangunan Dan Sokongan	
Memastikan keselamatan perisian sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal pelaksanaan perubahan melalui peraturan formal; b. Membuat semakan teknikal selepas perubahan sistem operasi bagi menjamin tiada impak negatif ke atas keselamatan operasi MPKB-BRI; c. Mengawal dan menghad perubahan ke atas perisian yang perlu sahaja; d. Menghalang semua peluang untuk kebocoran maklumat; dan e. Mengawal selia dan memantau pembangunan perisian oleh pihak luar dari semasa ke semasa.	Pentadbir Sistem ICT

PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Dasar Kesinambungan Perkhidmatan	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaianperkhidmatan yang berterusan kepada pelanggan.	
10.1 Pelan Kesinambungan Perkhidmatan	**Tanggungjawab**
Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk memastikan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan MPKB-BRI dan melindungi aktiviti daripada kesan bencana serta pemulihan perkhidmatan dalam tempoh yang ditetapkan. Perkara yang perlu diberi perhatian adalah seperti berikut: a. Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Merancang dan melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. Mendokumenkan proses dan prosedur yang telah dipersetujui; d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; dan e. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	ICTSO, Pentadbir Sistem ICT

PERKARA 11 PEMATUHAN

Pematuhan Dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MPKB-BRI.	
11.1 Pematuhan Dasar	**Tanggungjawab**
Setiap pengguna di MPKB-BRI hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MPKB-BRI, undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa.	Semua Pengguna MPKB-BRI
11.2 Keperluan Perundangan	
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MPKB-BRI: a. Keselamatan perlindungan secara am i. *Emergency (Essential Power) Act 1964;* ii. *Essential (Key Points) Regulations 1965;* iii. Perakuan Jawatankuasa mengkaji semula peraturan keselamatan Pejabat Tahun 1982; iv. Arahan Keselamatan Yang Dikuatkuasakan Melalui Surat Pekeliling Am Sulit Bil. 1 Tahun 1985; v. Arahan Jawatankuasa Tetap Sasaran Penting Bil. 1 Tahun 1985; vi. Arahan Tetap Sasaran Penting Yang Dikeluarkan Kepada Pihak Yang Terlibat Dalam Pengurusan Sasaran Penting Milik Kerajaan Dan Swasta Yang Diluluskan Oleh Jemaah Menteri Pada 13 Oktober 1993; dan vii. Surat Pekeliling Am Sulit Bil. 1 Tahun 1993 - Meningkatkan Kualiti Kawalan Keselamatan Perlindungan Di Jabatan-Jabatan Kerajaan.	Semua Pengguna MPKB-BRI

PERKARA 11 PEMATUHAN

b. Keselamatan dokumen i. *Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control);* ii. Akta Rahsia Rasmi 1972; iii. Akta Arkib Negara 2003; iv. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh; v. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (*espionage*); vi. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976; vii. Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Ketua Setiausaha Negara Melalui Surat M(R)10308/3/(45) Bertarikh 8 Mei 1987; dan viii. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R)200/55 Klt.7(21) Bertarikh 21 Ogos 1999.	Semua Pengguna MPKB-BRI

PERKARA 11 PEMATUHAN

c. Keselamatan fizikal bangunan i. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959; ii. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan; *iii. State Key Points;* iv. Surat Pekeliling Am Rahsia Bil.1 Tahun 1975 - Keselamatan Jabatan-jabatan Kerajaan; v. Surat Bil. KPKK/308/A (2) bertarikh 7/9/79 - Mencetak Pas-Pas Keselamatan dan Kad-Kad Pengenalan Kementerian/Jabatan; vi. Surat Pekeliling Am Bil 4 Tahun 1982 - Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan vii. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.	Semua Pengguna MPKB-BRI

PERKARA 11 PEMATUHAN

d. Keselamatan individu i. *Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidenti;* ii. *General Circular Memorandum*; iii. *Instruction On Positive Vetting Procedure;* iv. Surat Pekeliling Am Sulit Bil.1/1966 - Perkara Keselamatan Tentang Persidangan- Persidangan/ Perjumpaan/Lawatan Sambil Belajar Antarabangsa; v. Surat Pekeliling Tahun 1966 – Tapisan Keselamatan Terhadap Pakar/Penasihat Luar Negeri**;** vi. Surat Pekeliling Am Sulit Bil.1/1967 – Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka-mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam Perwakilan Rasmi Malaysia semasa melawat Negara-negara tabir Buluh dan Tabir besi; vii. Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 - Melaporkan Perjumpaan/ Percakapan Di Antara Diplomat/ Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota-Anggota Kerajaan; dan viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.	Semua Pengguna MPKB-BRI

PERKARA 11 PEMATUHAN

e. Keselamatan aset ICT i. Akta Tandatangan Digital 1997; i. Akta Jenayah Komputer 1997; ii. Akta Hak Cipta (Pindaan) 1997; iii. Akta Multimedia dan Telekomunikasi 1998; iv. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan; v. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT); vi. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi – Agensi Kerajaan; vii. *Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002;* dan viii. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005. ix. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam . x. Akta dan Peraturan-peraturan lain yang berkaitan.	Semua Pengguna MPKB-BRI