



DASAR KESELAMATAN ICT

BAHAGIAN HAL EHWAL UNDANG-UNDANG

VERSI 1.0

JANUARI 2008

KANDUNGAN

MUKA SURAT

TAFSIRAN

6

PENDAHULUAN

I. Pengenalan

9

II. Objektif

9

III. Skop

9

IV. Prinsip-Prinsip

9

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

Dasar Keselamatan ICT

12

1.1 Pelaksanaan Dasar

12

1.2 Penyebaran Dasar

12

1.3 Penyelenggaraan Dasar

12

1.4 Pengecualian Dasar

12

PERKARA 02 ORGANISASI KESELAMATAN

Struktur Organisasi Keselamatan

13

2.1 Ketua Pengarah BHEUU

131

2.2 Jawatankuasa Penyelaras Keselamatan ICT

13

2.2.1 Ketua Pegawai Maklumat (CIO)

13

2.2.2 Pegawai Keselamatan ICT (ICTSO)

14

2.2.3 Pengurus Komputer

15

2.2.4 Pentadbir Sistem ICT

16

2.2.5 Penyelaras ICT

17

2.3 Pengguna

17

2.4 Pihak Ketiga

18

PERKARA 03 KAWALAN DAN PENGELASAN ASET

Akauntabiliti Aset	19
3.1 Inventori Aset	19
3.2 Pengkelasan Maklumat	19
3.3 Pengendalian Maklumat	20

PERKARA 04 KESELAMATAN SUMBER MANUSIA

Keselamatan Sumber Manusia	21
4.1 Sebelum Berkhidmat	21
4.2 Dalam Perkhidmatan	21
4.3 Bertukar atau Tamat Perkhidmatan	22

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Keselamatan Kawasan	23
5.1 Perimeter Keselamatan Fizikal	23
5.2 Kawalan Masuk Fizikal	23

Keselamatan Aset ICT	24
5.3 Perkakasan	24
5.4 Dokumen	24
5.5 Media Storan	25

Keselamatan Persekitaran	26
5.6 Kawalan Persekitaran	26
5.7 Bekalan Kuasa	27
5.8 Prosedur Kecemasan	27
5.9 Keselamatan Kabel	27
5.10 Penyelenggaraan Peralatan ICT	28
5.11 Peminjaman Peralatan Untuk Kegunaan Di Luar Pejabat	28
5.12 Pengendalian Peralatan Luar Yang Dibawa Masuk	29
5.13 Pelupusan dan Kitar Semula Peralatan	29
5.14 <i>Clear Desk</i> dan <i>Clear Screen</i>	29

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

Pengurusan Prosedur Operasi	30
6.1 Pengendalian Prosedur	30
6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	30
6.3 Perancangan dan Penerimaan Sistem	31
6.4 Perlindungan dari Kod Jahat	32
6.5 <i>Housekeeping</i>	33
6.5.1 Penduaan	33
6.5.2 Sistem Log	33
Pengurusan Rangkaian	34
6.6 Kawalan Infrastruktur Rangkaian	34
Pengurusan Media	35
6.7 Penghantaran dan Pemindahan	35
6.8 Pengendalian Media	35
Keselamatan Komunikasi	36
6.9 Internet	36
6.10 Mel Elektronik	36

PERKARA 07 PENGURUSAN INSIDEN KESELAMATAN ICT

Menangani Insiden Keselamatan ICT	37
7.1 Prosedur Pengurusan Insiden	37
7.2 Pelaporan Insiden	37

PERKARA 08 KAWALAN CAPAIAN

Kawalan Capaian	38
8.1 Keperluan Dasar	38
8.2 Pengurusan Capaian Pengguna	39
8.3 Tanggungjawab Pengguna	39
8.4 Kawalan Capaian Rangkaian	40
8.5 Kawalan Capaian Sistem Operasi	41
8.6 Kawalan Capaian Aplikasi dan Maklumat	42

8.7	Penggunaan Peralatan ICT Mudah Alih	42
-----	-------------------------------------	----

PERKARA 09 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Perolehan, Pembangunan dan Penyelenggaraan Sistem dan Aplikasi 43

9.1	Keperluan Keselamatan	43
9.2	Kawalan Kriptografi	43
9.3	Kawalan Perisian Operasi	44
9.4	Keselamatan Dalam Proses Pembangunan dan Sokongan	44

PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Dasar Kesinambungan Perkhidmatan 45

10.1	Pelan Kesinambungan Perkhidmatan	45
------	----------------------------------	----

PERKARA 11 PEMATUHAN

Pematuhan dan Keperluan Perundangan 46

11.1	Pematuhan Dasar	46
11.2	Keperluan Perundangan	46

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 / Agensi	Termasuk Ketua Setiausaha, Ketua Pengarah, Timbalan Ketua Setiausaha, Timbalan-timbalan Ketua Pengarah, Setiausaha Bahagian, Pengarah Bahagian/Jabatan, Pengarah-pengarah Pelajaran Negeri, Pejabat Pelajaran Bahagian, Pejabat Pelajaran Daerah, Kolej, IPG dan Sekolah-sekolah.
Insiden Keselamatan	Musibah (<i>adverse event</i>) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.

TAFSIRAN

Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (<i>soft copy</i>), 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 BHEUU
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 BHEUU
Peralatan perlindungan	Peralatan yang berfungsi untuk pengawalan, pencegahan dan pengurusan tampalan seperti firewall, router, proxy, antivirus, dll
Insiden Keselamatan	Bermaksud musibah (<i>adverse event</i>) yang berlaku ke atas sistem maklumat
Enkripsi	Bermaksud menjadikan teks biasa (<i>plaintext</i>) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks <i>cipher</i> . 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.

TAFSIRAN

Pengguna Kakitangan BHEUU, pembekal, pakar runding, dll

Warga BHEUU Kakitangan BHEUU

PENDAHULUAN

I. Pengenalan

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang perlu dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) BAHAGIAN HAL EHWAL UNDANG-UNDANG (BHEUU). Dasar ini juga menerangkan kepada semua pengguna di BHEUU mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT BHEUU.

II. Objektif

Dasar Keselamatan ICT BHEUU diwujudkan untuk memastikan tahap keselamatan ICT BHEUU terus dan dilindungi bagi menjamin kesinambungan urusan BHEUU 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 BHEUU termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT BHEUU

IV. Prinsip-Prinsip

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT BHEUU 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;

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 mewujudkan, 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 BHEUU;

d. Pengasingan

Tugas mewujudkan, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperinci 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*, *Anti virus* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

f. Pematuhan

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

g. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan (*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
<p>Ketua Pengarah BHEUU adalah bertanggungjawab ke atas pelaksanaan arahan dengan dibantu oleh Jawatankuasa Penyelaras Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pengurus Komputer, Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.</p>	<p>Ketua Pengarah atau Pegawai yang diturunkan kuasa</p>
1.2 Penyebaran Dasar	
<p>Dasar ini bertujuan memastikan hala tuju pengurusan keselamatan kementerian untuk melindungi asset ICT selaras dengan keperluan perundangan.</p> <p>Dasar ini perlu disebar kepada semua pengguna BHEUU (termasuk kakitangan, pembekal, pakar runding dan lain-lain yang berurusan dengan BHEUU)</p>	<p>ICTSO</p>
1.3 Penyelenggaraan Dasar	
<p>Dasar Keselamatan ICT BHEUU adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan organisasi.</p> <p>Prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT BHEUU adalah seperti berikut:</p> <ol style="list-style-type: none"> 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. 	<p>ICTSO</p>
1.4 Pemakaian Dasar	
<p>Dasar Keselamatan ICT BHEUU adalah terpakai kepada semua pengguna ICT BHEUU dan tiada pengecualian diberikan.</p>	<p>Semua Pengguna BHEUU</p>

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 Ketua Pengarah BHEUU	Tanggungjawab
Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: <ul style="list-style-type: none"> a. Memastikan pelaksanaan Jawatankuasa Penyelaras Keselamatan ICT BHEUU; b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT BHEUU; 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 BHEUU. 	Ketua Setiausaha atau Pegawai yang diturunkan kuasa
2.2 Jawatankuasa Penyelaras Keselamatan ICT	
Objektif : Menerangkan peranan dan tanggungjawab ahli pasukan penyelaras keselamatan BHEUU	
2.2.1 Ketua Pegawai Maklumat (CIO)	Tanggungjawab
Peranan dan tanggung jawab CIO adalah seperti berikut: <ul style="list-style-type: none"> a. Mewujud dan mengetuai pasukan penyelaras keselamatan ICT BHEUU; b. Menasihati Ketua Pengarah BHEUU 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 BHEUU. 	

PERKARA 02 ORGANISASI KESELAMATAN

2.2.2 Pegawai Keselamatan ICT (ICTSO)	Tanggungjawab
<p>Peranan dan tanggungjawab ICTSO adalah seperti berikut:</p> <ul style="list-style-type: none">a. Mengurus program-program keselamatan ICT;b. Menguatkuasa dan memantau pematuhan keatas 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 tindak balas pengurusan BHEUU 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 memaklumpkannya 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 BHEUU; dank. Membangun, menyelaras dan melaksana pelan latihan dan program kesedaran keselamatan ICT.	CIO

PERKARA 02 ORGANISASI KESELAMATAN

2.2.3 Pengurus Komputer	Tanggungjawab
<p>Peranan dan tanggungjawab Pengurus Komputer adalah seperti berikut:</p> <ul style="list-style-type: none">a. Memahami dan mematuhi Dasar Keselamatan ICT BHEUU;b. Menentukan kawalan akses semua pengguna terhadap aset ICT BHEUU;c. Melaporkan sebarang perkara atau ancaman keatas keselamatan ICT kepada ICTSO; dand. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT BHEUU.	Penyelaras ICT
2.2.4 Pentadbir Sistem ICT	Tanggungjawab
<p>Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:</p> <ul style="list-style-type: none">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 BHEUU;c. Memastikan kerahsiaan katalaluan dan memantau aktiviti capaian harian pengguna;d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan serta merta;e. Menyimpan dan menganalisis rekod jejak audit (<i>audit trail</i>); danf. 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/ JPN/PPB/PPD/IPG/KM/Sekolah	Tanggungjawab
<p>Peranan dan tanggungjawab Penyelaras ICT adalah seperti berikut:</p> <ul style="list-style-type: none">a. Melaksanakan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT BHEUU;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 BHEUU kepada ICTSO; danf. Melaksanakan program-program kesedaran mengenai keselamatan ICT.	Penyelaras ICT

PERKARA 02 ORGANISASI KESELAMATAN

2.3 Pengguna ICT BHEUU	Tanggungjawab
<p>Pengguna adalah termasuk kakitangan BHEUU, pembekal, pakar runding dll. Peranan dan tanggungjawab pengguna adalah seperti berikut:</p> <ul style="list-style-type: none">a. Memahami dan mematuhi Dasar Keselamatan ICT BHEUU;b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;c. Melepassi tapisan keselamatan (jika berkaitan);d. Mematuhi prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat BHEUU;e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Penyelaras ICT dengan segera; danf. Menyertai program-program kesedaran mengenai keselamatan ICT.g. Mengambil langkah-langkah perlindungan seperti berikut :-<ul style="list-style-type: none">1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;2. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;3. Menentukan maklumat sedia untuk digunakan;4. Menjaga kerahsiaan kata laluan;5. Mematuhi standard, prosedur, langkah dan garis panduan yang ditetapkan;6. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, peprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan7. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua Pengguna BHEUU

PERKARA 02 ORGANISASI KESELAMATAN

2.4 Pihak Ketiga/luar	Tanggungjawab
<p>Keselamatan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga/ luar hendaklah sentiasa dikawal.</p> <p>Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai:</p> <ul style="list-style-type: none">a. Dasar Keselamatan ICT BHEUU;b. Tapisan Keselamatan;c. Perakuan Akta Rahsia Rasmi 1972;d. Hak Harta Intelek; <p>Nota 1:</p> <p>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.</p>	<p>Penyelaras ICT Jabatan/ Bahagian, Pentadbir Sistem ICT</p>

PERKARA 03 KAWALAN DAN PENGELASAN ASET

Akauntabiliti Aset	
Objektif : Memberi dan menyokong perlindungan yang optimum ke atas semua aset ICT BHEUU.	
3.1 Inventori Aset	Tanggungjawab
<p>Memastikan semua aset ICT BHEUU hendaklah diberi perlindungan yang bersesuaian oleh pemilik atau pemegang amanah masing-masing.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Memastikan semua asset dikenal pasti dan maklumat aset direkodkan dalam daftar harta modal dan inventori (TPA Kew 2) dan sentiasa kemaskini. b. Memastikan semua asset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan c. Mengenal pasti, mendokumen dan melaksanakan peraturan bagi penggunaan aset. 	Semua pengguna BHEUU
3.2 Pengkelasan Maklumat	
<p>Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan kepada tahap sensitiviti masing-masing.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal BHEUU. Setiap maklumat hendaklah dikelas dan dilabelkan mengikut sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: <ol style="list-style-type: none"> i. Rahsia Besar; ii. Rahsia; iii. Sulit; atau iv. Terhad. 	Pegawai yang diberi tanggungjawab

PERKARA 03 KAWALAN DAN PENGELASAN ASET

3.3 Pengendalian Maklumat	
<p>Pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penyalinan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut :</p> <ol style="list-style-type: none"> 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. 	<p>Semua Pengguna BHEUU</p>

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
<p>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, kecuiaan, kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 BHEUU
4.2 Dalam Perkhidmatan	
<p>Memastikan semua pengguna sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong dasar keselamatan ICT BHEUU.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Memastikan semua pengguna BHEUU mengurus keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh BHEUU; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan ICT diberi kepada semua pengguna BHEUU 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 BHEUU sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan oleh BHEUU. 	Semua Pengguna BHEUU

PERKARA 04 KESELAMATAN SUMBER MANUSIA

4.3 Bertukar Atau Tamat Perkhidmatan	
<p>Memastikan semua pengguna BHEUU yang tamat perkhidmatan atau bertukar dari BHEUU diurus dengan teratur.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none">a. Memastikan semua aset ICT Kerajaan dikembalikan kepada BHEUU mengikut peraturan dan/ atau terma yang ditetapkan oleh BHEUU; danb. Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh BHEUU.	Semua pengguna BHEUU

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
<p>Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>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;</p> <ol style="list-style-type: none"> a. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; b. Memperkukuhkan dinding dan siling; c. Memasang alat penggera atau kamera litar tertutup (CCTV), jika berkaitan; d. Menghadkan laluan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan g. Mewujudkan perkhidmatan kawalan keselamatan. 	CIO, ICTSO dan Penyelaras ICT
5.2 Kawalan Masuk Fizikal	
<p>Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis/ bangunan BHEUU.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 BHEUU

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 BHEUU.	
5.3 Perkakasan	
<p>Peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh berfungsi apabila diperlukan.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 agensi-agensi BHEUU. 	Semua Pengguna BHEUU
5.4 Dokumen	
<p>Langkah-langkah pengurusan dokumen yang baik dan selamat perlu dilaksanakan bagi memastikan integriti maklumat.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 BHEUU

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.5 Media Storan	Tanggungjawab
<p data-bbox="183 353 1149 584">Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat.</p> <p data-bbox="183 656 845 685">Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul data-bbox="236 757 1133 1189" style="list-style-type: none"><li data-bbox="236 757 1133 837">a. Menyediakan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;<li data-bbox="236 857 1133 938">b. Menghadkan akses untuk memasuki kawasan penyimpanan media kepada pengguna yang dibenarkan sahaja;<li data-bbox="236 958 1133 1088">c. Merujuk kepada tatacara pelupusan sekiranya penghapusan maklumat hendak dilakukan dan mestilah mendapat kebenaran pemilik maklumat terlebih dahulu; dan<li data-bbox="236 1108 1133 1189">d. Merekodkan pengurusan media termasuk inventori, pergerakan dan penduaan (<i>backup</i>).	Semua Pengguna BHEUU

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Keselamatan Persekitaran	
Objektif: Melindungi aset ICT BHEUU dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.	
5.6 Kawalan Persekitaran	Tanggungjawab
<p>Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubah suai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK).</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none">Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;Memasang peralatan perlindungan hendaklah di tempat yang bersesuaian, mudah dikenali dan dikendalikan;Menyimpan bahan mudah terbakar hendaklah di luar kawasan kemudahan penyimpanan aset ICT;Meletakkan semua bahan cecair hendaklah di tempat yang bersesuaian dan berjauhan dari aset ICT;Melarang engguna merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT; danMemeriksa 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 BHEUU

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.7 Bekalan Kuasa	Tanggungjawab
<p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>Menggunakan peralatan sokongan seperti UPS (Uninterruptable Power <i>Supply</i>) dan penjana (<i>generator</i>) bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan;</p> <ol style="list-style-type: none"> a. Memeriksa dan menguji semua peralatan sokongan bekalan kuasa secara berjadual; dan b. Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai. 	Ketua Jabatan/ Bahagian/ Unit
5.8 Prosedur Kecemasan	Tanggungjawab
<p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada prosedur kecemasan yang telah ditetapkan;</p> <ol style="list-style-type: none"> a. Melaporkan insiden kecemasan persekitaran dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ); b. Mengada, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa; dan c. Merancang dan mengadakan latihan kebakaran bangunan (<i>fire drill</i>) secara berkala. 	Semua Pengguna BHEUU
5.9 Keselamatan Kabel	Tanggungjawab
<p>Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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	Tanggungjawab
<p>Peralatan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti maklumat.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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	Tanggungjawab
<p>Peralatan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Mendapatkan kelulusan mengiku peraturan dibawah Pekeliling Perbendaharaan Tatacara Pengurusan Aset atau peraturan BHEUU 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. 	Ketua Bahagian/ Jabatan

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.12 Pengendalian Peralatan Luar Yang Dibawa Masuk	Tanggungjawab
<p>Bagi peralatan yang dibawa masuk ke premis kerajaan, perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT BHEUU; b. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh BHEUU bagi membawa masuk/ keluar peralatan; dan c. Memeriksa 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	
<p>Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan BHEUU:</p> <ol style="list-style-type: none"> a. Menghapuskan semua kandungan khususnya maklumat rahsia rasmi terlebih dahulu sama ada melalui <i>shredding</i>, <i>grinding</i>, <i>degauzing</i> atau pembakaran sebelum pelupusan; dan b. Merujuk kepada Pekeliling Perbendaharaan Bil. 5 Tahun 2007 "Tatacara Pengurusan Aset Alih Kerajaan. 	Semua Pengguna BHEUU
5.14 <i>Clear Desk</i> Dan <i>Clear Screen</i>	
<p><i>Clear Desk</i> dan <i>Clear Screen</i> bermaksud tidak meninggalkan bahan-bahan yang sensitive terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Menggunakan kemudahan <i>password screen saver</i> atau <i>logout</i> 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 BHEUU

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
<p>Memastikan kemudahan pemprosesan maklumat beroperasi seperti yang ditetapkan dan selamat.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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	
<p>Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 system dan proses yang terlibat serta penilaian semula risiko. 	Pentadbir Sistem ICT

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

<p>6.3 Perancangan Dan Penerimaan Sistem</p>	
<p>Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> 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. Menetapkan kriteria penerimaan untuk system maklumat baru, peningkatan dan versi baru dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan system; 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. 	<p>Pentadbir Sistem ICT</p>

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

6.4 Perlindungan Dari Kod Jahat (<i>Malicious Code</i>)	
<p>Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, <i>worm</i>, <i>trojan</i> dan <i>spyware</i>.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none">a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan <i>Intrusion Detection System (IDS)</i> 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 <i>pattern</i> 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; dani. Memberi amaran mengenai ancaman keselamatan ICT dari semasa ke semasa.	Semua Pengguna BHEUU

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

6.5 Housekeeping	
Mengekalkan integriti, kebolehsediaan maklumat dan kemudahan pemprosesan maklumat.	
6.5.1 Penduaan (<i>Backup</i>)	
<p>Bagi memastikan system dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan hendaklah direkodkan dan disimpan di lokasi yang berlainan.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Membuat salinan keselamatan ke atas semua system perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut kesesuaian operasi; 	Pentadbir Sistem ICT
6.5.2 Sistem Log	
<p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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

Pengurusan Rangkaian	
Objektif: Memastikan perlindungan keselamatan maklumat dalam rangkaian dan infrastruktur sokongan terus dan terkawal.	
6.6 Kawalan Infrastruktur Rangkaian	Tanggungjawab
<p>Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Membangun dan melaksanakan polisi dan prosedur bagi melindungi maklumat berhubung kait dengan system 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 <i>Factory Acceptance Check (FAC)</i> semasa pemasangan dan konfigurasi; g. Memastikan semua trafik rangkaian melalui firewall di bawah kawalan BHEUU; h. Memasang perisian <i>Intrusion Detection System (IDS)</i> bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat BHEUU; i. Memasang <i>Web Content Filter</i> pada <i>Internet Gateway</i> 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"; j. Mendapat kebenaran ICTSO bagi sebarang penyambungan rangkaian yang bukan di bawah kawalan BHEUU; 	Pentadbir Sistem ICT

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	Tanggungjawab
<p>Prosedur bertujuan mengendali dan menyimpan maklumat daripada didedah tanpa kebenaran atau disalah guna.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 BHEUU dan mana-mana agensi luar terjamin.
6.9 Internet	
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 BHEUU
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 BHEUU

PERKARA 07 PENGURUSAN INSIDEN KESELAMATAN ICT

Menangani Insiden Keselamatan ICT	
Objektif: Memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan serta meminimumkan kesan insiden keselamatan ICT.	
7.1 Prosedur Pengurusan Insiden	Tanggungjawab
<p>Prosedur pengurusan insiden perlu diwujudkan dan didokumentasikan.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identity dan pengubahsuaan perisian tanpa kebenaran; b. Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. Menyediakan pelan tindakan pemulihan segera. 	ICTSO
7.2 Pelaporan Insiden	Tanggungjawab
<p>Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO / Penyelaras Keselamatan ICT Jabatan/Bahagian dengan kadar segera.</p> <p>Insiden keselamatan ICT adalah termasuk yang berikut:</p> <ol style="list-style-type: none"> 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 mencerooboh, penyelewengan dan insiden-insiden yang tidak diingini. <p>Nota 2: Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT" mengenainya bolehlah dirujuk.</p>	Semua Pengguna BHEUU

PERKARA 08 KAWALAN CAPAIAN

Kawalan Capaian	
Objektif : Memahami dan mematuhi keperluan keselamatan dalam membuat capaian dan menggunakan aset ICT BHEUU.	
8.1 Keperluan Dasar	Tanggungjawab
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.	Semua Pengguna BHEUU
8.2 Pengurusan Capaian Pengguna	Tanggungjawab
<p>Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk membuat capaian maklumat dan perkhidmatan; b. Akaun pengguna adalah unik dan pengguna bertanggungjawab keatas 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: <ol style="list-style-type: none"> 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 	Pentadbir Sistem atau Penyelaras ICT

DASAR KESELAMATAN ICT BHEUU

<p>iv. Pengguna bertukar, berpindah agensi, bersara dan/atau tamat perkhidmatan.</p> <p>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.</p>	
8.3 Tanggungjawab Pengguna	Tanggungjawab
<p>Memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none">a. Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan;b. Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; danc. Mematuhi amalan <i>clear desk/ clear screen policy</i>.	Semua Pengguna BHEUU

PERKARA 08 KAWALAN CAPAIAN

8.4 Kawalan Capaian Rangkaian	Tanggungjawab
<p>Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.</p> <p>Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan menempatkan atau memasang antaramuka diantara rangkaian BHEUU dan lain-lain organisasi serta mewujudkan dan menguatkuasa mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none">a. Memastikan pengguna boleh membuat capaian ke atas perkhidmatan yang dibenarkan sahaja;b. Menggunakan kaedah pengenalan automatic berdasarkan lokasi dan peralatan untuk pengesahan sambungan ke dalam rangkaian;c. Mengawal capaian fizikal dan logical keatas kemudahan port diagnostic dan konfigurasi jarak jauh;d. Mengasingkan capaian mengikut kumpulan perkhidmatan maklumat, pengguna dan system maklumat dalam rangkaian;e. Mengawal sambungan ke rangkaian, khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan BHEUU; danf. Mewujud dan melaksana kawalan pengalihan laluan (routing control) untuk memastikan pematuhan ke atas peraturan BHEUU.	

PERKARA 08 KAWALAN CAPAIAN

8.5 Kawalan Capaian Sistem Operasi	
<p>Memastikan capaian ke atas system operasi dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja.</p> <p>Kaedah yang digunakan hendaklah mampu menyokong perkara berikut:</p> <ol style="list-style-type: none">a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan BHEUU;b. Mewujudkan <i>audit trail</i> ke atas semua capaian system operasi terutama pengguna bertaraf khas (<i>super user</i>);c. Menjada amaran (<i>alert</i>) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem;d. Menghadkan tempoh penggunaan mengikut kesesuaian. <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none">a. Mengawal capaian ke atas system operasi menggunakan prosedur <i>log-on</i> yang selamat;b. Prosedur lo-gon yang selamat perlulah:<ol style="list-style-type: none">i. Menggunakan kaedah pengenalan pengguna yang unik dan teknik pengesahan pengguna yang berkesan dan selamat;ii. Melaksana sisten pengurusan kata laluan yang interaktif dan menjamin kualiti serta keselamatan kata laluan;iii. Mengawal penggunaan utility yang berkeupayaan melepasi system dan aplikasi terhad;iv. Menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan; danv. Menghadkan tempoh masa penggunaan bagi meningkatkan keselamatan aplikasi yang berisiko tinggi.	

PERKARA 08 KAWALAN CAPAIAN

8.6 Kawalan Capaian Aplikasi Dan Maklumat	
<p>Capaian sistem dan aplikasi di BHEUU adalah terhad kepada pengguna dan tujuan yang dibenarkan sahaja.</p> <p>Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:</p> <ol style="list-style-type: none"> 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 utility yang sedia ada dalam system operasi dan perisian malicious yang berupaya melangkaui kawalan sistem. <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Membuat capaian ke atas maklumat dan fungsi system aplikasi oleh pengguna perlu dihadkan, selaras dengan peraturan BHEUU; dan b. Mengasingkan persekitaran pengkomputeran yang khusus bagi sistem yang sensitif. 	<p>Pentadbir Sistem ICT</p>
8.7 Penggunaan Peralatan ICT Mudah Alih	
<p>Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan ICT mudah alih.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 jauh adalah sesuai dan selamat. 	<p>Pentadbir Sistem ICT</p>

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
<p>Memastikan kawalan keselamatan yang sesuai dijalinkan ke dalam aplikasi bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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. 	<p>Pemilik sistem, Pentadbir Sistem ICT, ICTSO</p>
9.2 Kawalan Kriptografi	
<p>Memastikan kaedah kriptografi diguna untuk melindungi kerahsiaan, kesahihan dan integriti maklumat.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 BHEUU. 	<p>Pentadbir Sistem ICT</p>

PERKARA 09 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

9.3 Kawalan Perisian Operasi	
<p>Memastikan kaedah yang sesuai dilaksanakan untuk mengawal capaian ke atas fail system dan kod sumber program bagi menjamin keselamatan system fail.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none">Mewujudkan peraturan untuk mengawal pemasangan perisian ke dalam persekitaran operasi;Mewujudkan peraturan untuk pemilihan, perlindungan dan kawalan data ujian; danMengawal dan menghadkan capaian ke atas kod sumber kepada pengguna yang dibenarkan sahaja.	Pentadbir Sistem ICT
9.4 Keselamatan Dalam Proses Pembangunan Dan Sokongan	
<p>Memastikan keselamatan perisian system aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan.</p> <p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none">Mengawal pelaksanaan perubahan melalui peraturan formal;Membuat semakan teknikal selepas perubahan sistem operasi bagi menjamin tiada impak negatif ke atas keselamatan operasi BHEUU;Mengawal dan menghad perubahan ke atas perisian yang perlu sahaja;Menghalang semua peluang untuk kebocoran maklumat; danMengawal 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 penyampaian perkhidmatan yang berterusan kepada pelanggan.	
10.1 Pelan Kesinambungan Perkhidmatan	Tanggungjawab
<p>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 BHEUU dan melindungi aktiviti daripada kesan bencana serta pemulihan perkhidmatan dalam tempoh yang ditetapkan.</p> <p>Perkara yang perlu diberi perhatian adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 BHEUU.	
11.1 Pematuhan Dasar	Tanggungjawab
Setiap pengguna di BHEUU hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT BHEUU, undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.	Semua Pengguna BHEUU
11.2 Keperluan Perundangan	
<p>Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di BHEUU:</p> <p>a. Keselamatan perlindungan secara am</p> <ol style="list-style-type: none"> i. <i>Emergency (Essential Power) Act 1964;</i> ii. <i>Essential (Key Points) Regulations 1965;</i> 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 BHEUU

PERKARA 11 PEMATUHAN

<p>b. Keselamatan dokumen</p> <ul style="list-style-type: none"> i. <i>Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control)</i>; 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 (<i>espionage</i>); 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 PengarahNegara 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. 	<p>Semua Pengguna BHEUU</p>
--	-----------------------------

PERKARA 11 PEMATUHAN

<p>c. Keselamatan fizikal bangunan</p> <ul style="list-style-type: none">i. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959;ii. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan;iii. <i>State Key Points</i>;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; danvii. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.	<p>Semua Pengguna BHEUU</p>
--	-----------------------------

PERKARA 11 PEMATUHAN

<p>d. Keselamatan individu</p> <ul style="list-style-type: none">i. <i>Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidential;</i>ii. <i>General Circular Memorandum;</i>iii. <i>Instruction On Positive Vetting Procedure;</i>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; danviii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.	<p>Semua Pengguna BHEUU</p>
---	-----------------------------

PERKARA 11 PEMATUHAN

<p>e. Keselamatan aset ICT</p> <ul style="list-style-type: none">i. Akta Tandatangan Digital 1997;ii. Akta Jenayah Komputer 1997;iii. Akta Hak Cipta (Pindaan) 1997;iv. Akta Multimedia dan Telekomunikasi 1998;v. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;vi. Pekeliling Am Bil. 1 Tahun 2001 –Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT);vii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi – Agensi Kerajaan;viii. <i>Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002</i>; danix. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.x. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam .xi. Akta dan Peraturan-peraturan lain yang berkaitan.	<p>Semua Pengguna BHEUU</p>
---	---------------------------------