MEMO PERHUBUNGAN
BAHAGIAN HAL EHWAL UNDANG-UNDANG

Ruj. Kami: BHEUU.100-1/5/1 ( )	Tarikh: 28 Mei 2019
Kepada : P(Pembangunan) P(Dasar) P(Kewangan) P(PSM) P(PM) PUU K(KK) PP(IN) PT(Seksyen)	Salinan Kepada: YBhg. Dato' KP YBrs. TKP(D&P) YBrs. TKP(U)
Daripada : PPTK(PSM)KP	
Perkara : **GARIS PANDUAN KESELAMATAN PEJABAT BAHAGIAN HAL EHWAL UNDANG-UNDANG**	

Tuan/Puan,

Dengan hormatnya saya merujuk kepada perkara di atas.

2. Dimaklumkan Mesyuarat Keselamatan Jabatan pada 8 Mei 2019 yang di pengerusikan oleh TKP(U) telah bersetuju supaya 'Garis Panduan Keselamatan Pejabat Bahagian Hal Ehwal Undang-Undang' di edarkan semula kepada semua seksyen/unit untuk makluman dan perhatian selanjutnya. Garis Panduan Keselamatan sebelum ini telah diluluskan dan diedarkan kepada semua warga BHEUU, JBG dan MdI pada 05 Disember 2013.

3. Bersama-sama ini dilampirkan Garis Panduan Keselamatan Pejabat sebagai panduan dan peringatan bagi meningkatkan lagi kualiti keselamatan perlindungan di Bangunan Bahagian Hal Ehwal Undang-Undang.

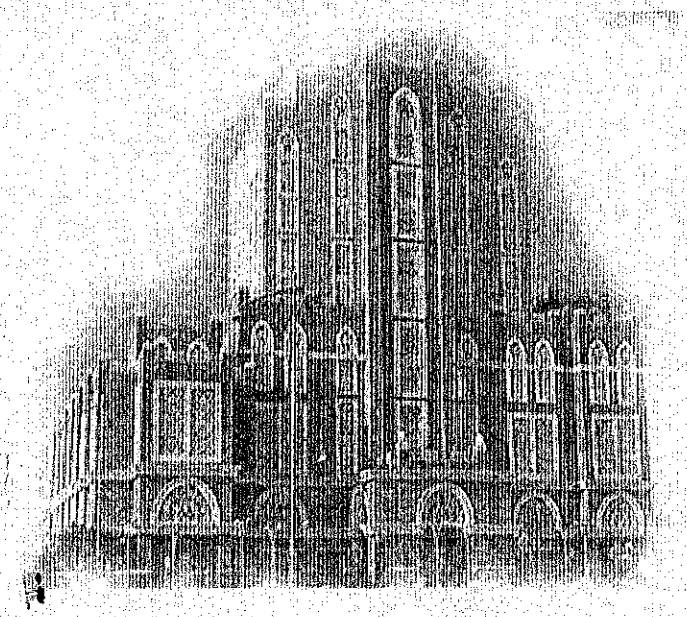
Sekian, terima kasih.

'BERKHIDMAT UNTUK NEGARA'

(SELAMAT BIN BUANG)

100-1/5/1.

GARIS PANDUAN KESELAMATAN PEJABAT



BAHAGIAN HAL EHWAL UNDANG-UNDANG

JABATAN PERDANA MENTERI

Disember 2013

BHEUU/ 06/(S) 349

GARIS PANDUAN KESELAMATAN PEJABAT BAHAGIAN HAL EHWAL UNDANG-UNDANG

TUJUAN

Garis Panduan Keselamatan ini dikeluarkan sebagai panduan bagi meningkatkan lagi kualiti keselamatan perlindungan di Bahagian Hal Ehwal Undang-Undang (BHEUU). Garis Panduan ini hendaklah dibaca bersekali dengan Dokumen Arahan Keselamatan yang dikeluarkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan.

Garis Panduan Keselamatan Pejabat BHEUU ini dibahagikan kepada empat (4) bahagian iaitu **Keselamatan Fizikal, Keselamatan Dokumen, Keselamatan Peribadi** dan **Keselamatan ICT.**

A. KESELAMATAN FIZIKAL

1. Mengadakan lampu kecemasan serta menghadkan pintu keluar masuk.

2. Memasang sistem pencegahan dan keselamatan kebakaran dalam bangunan mengikut spesifikasi yang diperakui oleh Jabatan Bomba dan Penyelamat Malaysia.

3. Memasang sistem siar raya, penggera keselamatan, kamera litar tertutup (CCTV) dan lain-lain kelengkapan keselamatan bagi tujuan memberi hebahan kepada warga bangunan.

4. Mengadakan Pengawal Keselamatan yang dilengkapi dengan alat-alat keselamatan. Tugas-tugas Pengawal Keselamatan ialah seperti berikut:

   4.1 mengadakan kawalan keselamatan dan rondaan di bangunan pejabat;

   4.2 mengawasi setiap pergerakan atau aktiviti yang berlaku di dalam atau luar bangunan secara fizikal atau dari bilik CCTV; dan

   4.3 menyediakan laporan keselamatan harian dan mingguan.

4. Melaksanakan sistem pegawai bertugas yang bertanggungjawab terhadap keselamatan kepada Pegawai Keselamatan Jabatan dan Ketua Jabatan.

5. Mewujudkan Sistem Pas Keselamatan.

5.1 Mengeluarkan Pas Keselamatan untuk memasuki pejabat berdasarkan kategori berikut:
   a) Pas Keselamatan Tetap (untuk anggota jabatan);
   b) Pas Keselamatan Sementara; dan
   c) Pas Keselamatan Pelawat

5.2 Setiap anggota dikehendaki sentiasa memakai Pas Keselamatan ketika berada di pejabat dan pas tersebut dipulangkan setelah anggota meletakkan jawatan, tamat kontrak,bersara pilihan atau bersara wajib;

5.3 Pas Keselamatan Pelawat hendaklah dihadkan kepada Aras yang pelawat tersebut berurusan dan ianya hendaklah dikembalikan selepas tamat lawatan; dan

5.4 Kehilangan Pas Keselamatan hendaklah dilaporkan dengan serta merta kepada pejabat yang mengeluarkan Pas Keselamatan tersebut untuk tindakan penyahaktifan. Pas Keselamatan yang baru akan dikeluarkan dalam tempoh (2) hari selepas dokumen/butiran lengkap diterima.

6. Menyediakan Kaunter Pelawat dan tempat khas untuk pelawat berurusan.

7. Memastikan tingkap dan pintu diperkukuhkan dan dilengkapi dengan kunci keselamatan. Pegawai Keselamatan Jabatan hendaklah:

7.1 Bertanggungjawab ke atas semua perkara berkaitan dengan kunci dan anak kunci termasuk kunci-kunci keselamatan (kunci bilik fail, kunci kabinet, kunci peti besi dan sebagainya) yang ada dalam simpanannya;

7.2 Menyelenggarakan sebuah Buku Daftar Kunci yang mengandungi senarai lengkap kesemua anak kunci yang digunakan serta mengemaskinikannya dan membuat audit ke atas kunci-kunci tersebut setiap tiga (3) bulan;

7.3 Memastikan supaya anggota yang diamanahkan dengan kunci-kunci keselamatan bertanggungjawab sepenuhnya terhadap keselamatan kunci-kunci tersebut;

7.4 Memastikan supaya anak kunci termasuk kunci-kunci pendua tidak dilabel dan ditandakan dengan nama dan tempat dimana anak kunci itu akan digunakan. Hanya kod sahaja yang boleh digunakan untuk melabel anak kunci jika perlu;

7.5 Memastikan supaya anak kunci termasuk kunci pendua disimpan di dalam peti keselamatan yang berkunci dan peti keselamatan tersebut

hendaklah disimpan di dalam bilik anggota yang bertanggungjawab terhadap kunci-kunci tersebut;

7.6 Buku pergerakan anak kunci hendaklah diwujudkan bagi merekodkan pergerakan anak kunci tersebut. Pergerakan kunci perlu direkod dengan butiran seperti tarikh, nama, waktu dan tandatangan anggota yang mengambil kunci tersebut;

7.7 Memastikan supaya anak kunci pendua tambahan tidak sekali-kali boleh dibuat tanpa kebenaran;

7.8 Memastikan supaya peti besi diselenggara dengan betul. Nombor kombinasi peti besi hendaklah ditukar setahun sekali dan disalinkan kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK) atau apabila anggota yang mengetahui nombor kombinasi tersebut telah bertukar/berhenti atau apabila telah mengesyaki bahawa nombor kombinasi peti besi tersebut telah diketahui;

7.9 Memastikan supaya setiap anggota yang bertukar atau berhenti menyerahkan balik kesemua anak kunci yang ada di dalam simpanannya; dan

7.10 Kehilangan anak kunci keselamatan hendaklah dilaporkan segera kepada Pegawai Keselamatan Jabatan atau Ketua Jabatan yang akan menyiasat kehilangan tersebut dan mengemukakan laporan kepada Pegawai Keselamatan Kerajaan dalam masa 24 jam.

8. Memastikan serta mengawasi penggunaan mesin penyalin terutama sekali apabila membuat salinan dokumen terperingkat.

8.1 Seorang pegawai yang bertanggungjawab bagi mengawasi mesin-mesin penyalin hendaklah dilantik serta sebuah buku daftar hendaklah diadakan untuk merekodkan penggunaannya;

8.2 Semua mesin penyalin hendaklah disimpan dalam bilik yang berkunci atau lokasi yang selamat dan terkawal;

8.3 Hanya anggota yang dibenarkan sahaja boleh ditugaskan untuk membuat salinan dokumen terperingkat;

8.4 Memastikan jumlah salinan yang dibuat ialah jumlah yang diluluskan sahaja dan semua salinan yang rosak/tidak diperlukan hendaklah dirincih *(shred)* atau dimusnahkan;

8.5 Semakan ke atas buku daftar hendaklah dibuat setiap bulan untuk menentukan semua salinan dokumen terperingkat adalah dibuat mengikut peraturan; dan

8.6 Semua penyelewengan dan penyalahgunaan ke atas mesin penyalin hendaklah dilaporkan kepada Ketua Jabatan.

8.7 Memastikan sebarang data/memori dalam *hard disk* dipadam sepenuhnya sebelum dikembalikan kepada kontraktor penyewaan mesin penyalin.

9. Mengawal penggunaan telefon bimbit di dalam kawasan pejabat. Sehubungan itu, perkara berikut hendaklah diambil perhatian:

9.1 Semua anggota BHEUU, MdI dan JBG dikehendaki mematikan/ menukarkan telefon bimbit kepada mode 'silent' apabila berada dalam mesyuarat di Bangunan BHEUU.

B. KESELAMATAN DOKUMEN

10. Sistem Pergerakan Fail seperti Kad Indeks, Sistem Doket dan lain-lain sistem hendaklah diwujudkan untuk mengesan dan merekodkan pergerakan fail bagi mengatasi masalah kehilangan fail. Sehubungan itu, perkara-perkara berikut hendaklah dilaksanakan :

10.1 Fail terperingkat, dokumen sebut harga/tender, soalan peperiksaan dan lain-lain dokumen terperingkat disimpan dalam Kabinet Keluli Berpalang dan Berkunci serta/atau disimpan di Bilik Kebal. Dokumen rasmi yang tidak terperingkat hendaklah disimpan dalam kabinet keluli yang berkunci atau *Mobile Filling Cabinet* yang berkunci;

10.2 Bagi fail-fail Rahsia Besar, Rahsia yang mengandungi kertas-kertas Jemaah Menteri dan kes-kes terkelas hanya Pegawai Kumpulan Profesional dan Pengurusan (P&P) sahaja yang dibenarkan untuk menggunakan fail berkenaan. Pegawai/jabatan lain yang ingin menggunakannya hendaklah mendapatkan kebenaran bertulis daripada Ketua Pengarah/Timbalan Ketua Pengarah BHEUU/MdI/JBG;

10.3 Hanya pegawai di Gred 41 dan ke atas sahaja yang dibenarkan mengendalikan Fail Rahsia/Rahsia Besar. Bagi pegawai di Gred 38 dan ke bawah, mereka hendaklah mendapat kebenaran bertulis daripada Ketua Jabatan/Timbalan Ketua Jabatan;

10.4 Hanya anggota yang telah menandatangani Lampiran D Akta Rahsia Rasmi 1972 dan lulus tapisan keselamatan dibenarkan menguruskan dokumen terperingkat;

10.5 Bilik Fail hendaklah dikunci pada setiap masa. Segala urusan hendaklah melalui Kaunter Bilik Fail sahaja. Notis "DILARANG MASUK TANPA KEBENARAN" hendaklah ditampal di pintu masuk Bilik Fail dan pintu di mana dokumen terperingkat disimpan. Hanya anggota yang bertugas di Bilik Fail sahaja dibenarkan memasuki bilik berkenaan;

10.6 Penghantaran fail terperingkat hendaklah menggunakan beg berkunci;

10.7 Dokumen/Fail Rahsia Besar, Rahsia, Sulit atau Terhad yang hendak dibawa keluar daripada pejabat untuk tujuan rasmi hendaklah mendapat kebenaran daripada Ketua Jabatan; dan

10.8 Buku Rekod Keluar/Masuk Surat, Buku *Despatch* dan lain-lain buku yang berkaitan dengan urusan surat-menyurat hendaklah dikemas kini dan dipantau setiap masa oleh pegawai yang dilantik secara bertulis bertujuan untuk mengesan jika berlaku sebarang kehilangan surat-surat.

C. KESELAMATAN PERIBADI/PERSONEL

11. Setiap anggota yang dikehendaki akses kepada perkara-perkara terperingkat hendaklah menandatangani borang akuan Lampiran 'D' seperti terkandung dalam Arahan Keselamatan. Borang tersebut juga dikehendaki ditandatangani setiap tahun untuk tujuan peringatan. Sehubungan itu, perkara-perkara berikut hendaklah dilaksanakan:

11.1 Setiap anggota hendaklah menandatangani borang perakuan Lampiran 'E' seperti yang terkandung dalam Arahan Keselamatan sebelum berhenti/meninggalkan perkhidmatan Kerajaan;

11.2 Setiap anggota yang terlibat dengan maklumat terperingkat Rahsia Besar dan Rahsia hendaklah membuat Tapisan Keselamatan Halus, manakala anggota yang terlibat dengan perkara Sulit/Terhad sahaja termasuk orang awam yang ditempatkan secara sementara dikehendaki membuat Tapisan Keselamatan Kasar;

11.3 Ketua Jabatan adalah bertanggungjawab menyelenggarakan fail mengandungi satu senarai yang lengkap dan kemas kini mengenai

semua Jawatan Keselamatan Berjadual dan senarai pemegang jawatan tersebut; dan

11.4 Ketua Jabatan hendaklah memastikan keputusan Tapisan Keselamatan anggota direkodkan dalam Buku Perkhidmatan anggota berkenaan.

D. KESELAMATAN ICT

12. Setiap anggota yang bertanggungjawab untuk melaksanakan tugas serta program yang melibatkan ICT hendaklah mematuhi garis panduan yang ditetapkan bagi memastikan aset ICT sama ada peralatan dan maklumat dilindungi, dipelihara serta terjamin dari segi integriti, kerahsiaan dan kesahihannya. Keselamatan ICT yang diberi perhatian meliputi keselamatan fizikal dan maklumat terutamanya yang melibatkan peralatan mudah alih. Garis panduan yang perlu dipatuhi adalah seperti berikut:

12.1 Semua warga BHEUU, MdI dan JBG bertanggungjawab untuk memastikan keselamatan aset Kerajaan dan peralatan ICT yang dimiliki, di bawah jagaan dan kawalannya sentiasa terjamin.

12.2 Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan komputer.

12.3 Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT.

12.4 Pengguna dilarang sama sekali menukar set peralatan komputer yang dibekalkan selain yang dinyatakan dalam borang harta modal Kew.PA 2.

12.5 Komputer riba dan peralatan mudah alih milik Kerajaan hendaklah dikawal secara maksimum, disimpan dan dikunci di tempat yang selamat apabila tidak digunakan termasuk simpanan di pejabat, di luar pejabat atau di rumah. Oleh itu, pengguna dilarang keras meninggalkan komputer riba dalam kenderaan kerana ia boleh dikesan dengan alat khas oleh pihak yang tidak bertanggungjawab. Pengguna juga dinasihatkan tidak meninggalkan komputer riba di rumah. Sebaliknya ia hendaklah disimpan di tempat yang selamat di pejabat.

12.6 Penggunaan komputer riba hendaklah dikawal dengan pengenalan pengguna *(user id)* dan kata laluan *(password)*.

12.7 Bagi perkakasan yang dikongsi, aktiviti keluar masuk penggunaan peralatan hendaklah direkodkan dalam buku daftar khas dan dipertanggungjawabkan kepada seorang anggota bahagian bagi mengesan kehilangan atau pun kerosakan. Oleh itu, aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan dalam buku daftar khas. Peminjam bertanggungjawab untuk memulangkan perkakasan yang dipinjam dan memastikan ia dalam keadaan sempurna sebagaimana semasa ia dipinjam. Sebarang kerosakan disebabkan penggunaan semasa tempoh pinjaman hendaklah dimaklumkan semasa pengembalian.

12.8 Bagi pinjaman komputer riba, peminjam bertanggungjawab menghapuskan semua fail dokumen yang disediakan atau diwujudkan oleh mereka sebelum ia dikembalikan.

12.9 Perkakasan ICT yang dipinjam untuk kegunaan di luar pejabat terdedah kepada pelbagai risiko. Oleh itu, peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan berjawatan Ketua Seksyen dan ke atas, dan tertakluk kepada tujuan yang dibenarkan.

12.10 Semua warga jabatan dilarang menggunakan komputer riba, *thumbdrive*, disket, CD, *external hardisk* dan mana-mana media komputer mudah alih milik persendirian untuk menyimpan maklumat terperingkat jabatan kecuali dengan kebenaran Ketua Jabatan atau Pengurusan Tertinggi jabatan.

12.11 Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Oleh itu, konsep *clear desk* dan *clear screen* hendaklah diamalkan di mana warga jabatan tidak meninggalkan bahan-bahan sensitif terdedah sama ada atas meja atau paparan skrin komputer apabila tidak berada di tempat masing-masing walau pun seketika. Langkah-langkah berikut hendaklah diambil:

a) Log keluar komputer apabila meninggalkan komputer;
b) Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail berkunci; dan
c) Dokumen-dokumen yang mengandungi bahan-bahan sensitif hendaklah diambil segera dari pencetak.

12.12 Setiap anggota BHEUU, MdI dan JBG dilarang keras membawa keluar maklumat Jabatan sama ada melalui komputer mudah alih, *thumbdrive*, disket dan lain-lain media mudah alih milik persendirian

kecuali mendapat kebenaran terlebih dahulu dari Ketua Bahagian atau Pengurusan Tertinggi jabatan.

12.13 Semua pengguna dibenarkan menggunakan rangkaian yang disediakan oleh BHEUU sahaja. Penggunaan modem atau USB modem milik persendirian dilarang sama sekali di premis jabatan.

12.14 Media komputer mudah alih seperti *thumbdrive* dan disket hendaklah diimbas *(scan)* sebelum digunakan.

12.15 Semua pengguna dilarang sama sekali melakukan sebarang aktiviti yang melanggar tata cara penggunaan internet seperti memuat naik, memuat turun, menyimpan dan menggunakan perisian yang tidak berlesen dan perisian berbentuk hiburan seperti permainan elektronik *(game)*. Sila rujuk Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 : "Garis Panduan Mengenai Tatacara Penggunaan Internet Dan Mel Elektronik di Agensi-Agensi Kerajaan".

12.16 Pengguna hendaklah mematuhi tatacara penggunaan Internet dan e-mel yang telah ditetapkan agar keselamatan ke atas pemakaiannya akan terus terjamin. Peranan dan tanggungjawab pengguna adalah seperti berikut:

a) menggunakan akaun atau alamat e-mel yang diperuntukkan oleh jabatan;

b) memaklumkan kepada pentadbir sistem ICT dengan segera sekiranya mengesyaki akaun telah disalahgunakan;

c) menggunakan kata laluan yang baik dengan ciri-ciri keselamatan yang bersesuaian, iaitu seperti berikut:

i. Rahsiakan kata laluan anda dari pengetahuan orang lain. Pendedahan kepada yang tidak berhak adalah satu kesalahan di bawah Akta Jenayah Komputer 1997.
ii. Sekiranya kata laluan telah dikompromi atau disyaki dikompromi, hendaklah dilaporkan kepada pentadbir sistem ICT dan kata laluan sedia ada diubah dengan serta merta.
iii. Kata laluan hendaklah diubah secara berkala sekurang-kurangnya sekali dalam 30 hari.
iv. Kata laluan hendaklah mempunyai saiz sekurang-kurangnya lapan (8) aksara dengan gabungan alphanumerik dan simbol khas.

v. Elakkan dari menggunakan semula empat (4) kata laluan yang terdahulu.

vi. Kata laluan hendaklah dihafal dan jangan sekali-kali disalin di mana-mana media.

d) memastikan setiap fail yang dimuat turun bebas dari virus sebelum digunakan;

e) bertanggungjawab sepenuhnya terhadap semua kandungan fail elektronik termasuk e-mel di dalam akaun sendiri. Dengan itu, pengguna perlu bertindak bijak, profesional dan berhati-hati apabila berkomunikasi menerusi saluran elektronik;

f) berhenti dan memutuskan talian dengan serta-merta sekiranya kakitangan menerima dan disambungkan ke laman Internet yang mengandungi unsur-unsur tidak menyenangkan dan negatif;

g) mengadakan salinan atau penduaan pada media storan kedua elektronik seperti *thumbdrive* dan sebagainya bagi tujuan keselamatan;

h) memastikan kemudahan e-mel digunakan dan dibiarkan aktif pada keseluruhan waktu bekerja supaya e-mel yang dialamatkan sampai tepat pada masanya dan tindakan ke atasnya dapat disegerakan;

i) menggunakan kemudahan *password screen saver* atau log keluar apabila hendak meninggalkan komputer;

j) memaklumkan kepada pentadbir sistem ICT sekiranya berada di luar pejabat dalam tempoh waktu yang panjang, bercuti atau bertukar tempat kerja bagi memudahkan penyelenggaraan dilakukan; dan

k) memaklumkan kepada pentadbir sistem ICT atau pegawai keselamatan ICT (ICTSO) sekiranya berlaku atau mengesyaki berlakunya insiden keselamatan ICT.

12.17 Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada Pegawai Keselamatan ICT (ICTSO) dengan kadar segera:

a) Maklumat didapati hilang, didedahkan kepada 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 *(password)* hilang atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;

d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.

PENUTUP

Memelihara dan melindungi pelbagai aspek keselamatan Jabatan adalah merupakan tanggungjawab setiap anggota BHEUU, MdI dan JBG. Justeru itu, bagi memastikan ia dilaksanakan dengan sempurna semua anggota BHEUU, MdI dan JBG hendaklah sentiasa merujuk kepada Garis Panduan yang disediakan ini. Untuk kemudahan rujukan yang berterusan, Garis Panduan ini juga boleh diakses di laman web.

Disediakan oleh :

Unit Khidmat Pengurusan
Bahagian Hal Ehwal Undang-Undang
Jabatan Perdana Menteri

Diluluskan oleh :

DATO' HAJI ISMAIL BIN IBRAHIM
Ketua Pengarah
Bahagian Hal Ehwal Undang-Undang
Jabatan Perdana Menteri

5 **Disember 2013**