KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 4 TAHUN 2006

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) SEKTOR AWAM

JABATAN PERDANA MENTERI
MALAYSIA

9 November 2006

Dikelilingkan Kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Badan Berkanun Persekutuan
Semua Ketua Pengurusan Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI MALAYSIA
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN
PERSEKUTUAN
62502 PUTRAJAYA

Telefon : 603-88881957
Faks : 603-88883721

Rujukan Kami : UPTM(S) 159/338/6
Jld. 3 (3)

Tarikh : 9 November 2006

Semua Ketua Setiausaha Kementerian

Semua Ketua Jabatan Persekutuan

Semua Y.B. Setiausaha Kerajaan Negeri

Semua Ketua Pengurusan Badan Berkanun Persekutuan

Semua Ketua Pengurusan Pihak Berkuasa Tempatan

SURAT PEKELILING AM BILANGAN 4 TAHUN 2006

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) SEKTOR AWAM

TUJUAN

Surat Pekeliling Am ini bertujuan memperkemaskan pengurusan pengendalian insiden keselamatan ICT bagi sektor awam.

LATAR BELAKANG

2. Kerajaan telah mengeluarkan Pekeliling Am Bilangan 1 Tahun 2001 Mekanisme Pelaporan Insiden Keselamatan ICT yang berkuatkuasa mulai 4 April 2001 menjelaskan mekanisme pelaporan insiden keselamatan ICT di sektor awam bagi membolehkan *Government Computer Emergency Response Team* (GCERT) yang berpusat di MAMPU mendapat maklumat untuk menyediakan bantuan teknikal kepada agensi terlibat. Pekeliling ini juga merangkumi tanggungjawab GCERT MAMPU, agensi pelapor serta proses kerja pelaporan insiden keselamatan ICT agensi yang terlibat.

3. Memandangkan serangan siber berpotensi memberi implikasi keselamatan ke atas aset ICT dan sistem penyampaian kerajaan, maka Kerajaan bersetuju supaya mekanisme pelaporan insiden dalam Surat Pekeliling ini diperkemaskan di mana usaha menangani serangan siber ke atas infrastruktur ICT kerajaan perlu ditangani dengan bijak bagi memastikan sistem ICT kerajaan dapat beroperasi dengan baik tanpa gangguan.

PENUBUHAN PASUKAN PENGENDALI INSIDEN PERINGKAT AGENSI

4. Sebagai langkah memperkemaskan pengurusan pengendalian insiden keselamatan ICT, semua agensi yang melaksanakan infrastruktur ICT bagi membolehkan kerajaan berfungsi dan menyedia perkhidmatan sistem penyampaian, hendaklah menubuhkan pasukan pengendali insiden (CERT) di agensi masing-masing. CERT Agensi akan bertindak sebagai *first level support* kepada GCERT MAMPU dalam mengendali insiden keselamatan ICT, mengawasi dan memberi nasihat berkaitan keselamatan ICT kepada agensi-agensi di bawah kawalannya.

PANDUAN PENGURUSAN PENGENDALIAN INSIDEN

5. Bagi menjelaskan pengurusan pengendalian insiden ini, dua (2) dokumen disediakan iaitu Garis Panduan Pengurusan Pengendalian Insiden Keselamatan ICT Sektor Awam dan Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT CERT Agensi. Garis Panduan Pengurusan Pengendalian Insiden Keselamatan ICT Sektor Awam mengandungi perkara-perkara berikut :

(a) Perihal mengenai Insiden dan Jenis Insiden Keselamatan ICT;

(b) Tahap Keutamaan Tindakan Ke Atas Insiden;

(c) Penubuhan CERT Agensi;

(d) Tanggungjawab Ketua Jabatan;

(e) Tanggungjawab CERT Agensi;

(f) Tanggungjawab GCERT MAMPU; dan

(g) Proses Pelaporan Insiden Keselamatan ICT Sektor Awam

6. Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT CERT Agensi pula mengandungi proses terperinci dalam pengendalian insiden keselamatan ICT iaitu :

(a) Pentadbiran *Incident Response Handling* (IRH);

(b) Pengurusan Pengendalian Insiden;

(c) Penyebaran Maklumat;

(d) Penyelarasan Pengurusan Insiden;

(e) Panduan Komunikasi Pengendalian Insiden Secara Jarak Jauh;

(f) Template Borang IRH 1.0 : Maklumat Pengendalian Insiden Keselamatan ICT;

(g) Template Borang IRH 1.1 : Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT;

(h) Template Laporan Analisis Fail Log;

(i) Template Laporan Imbasan Hos; dan

(j) Template Laporan Kronologi Insiden Keselamatan ICT.

Garis Panduan Pengurusan Pengendalian Insiden Keselamatan ICT Sektor Awam dan Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT CERT Agensi adalah masing-masing seperti di **Lampiran 1** dan **Lampiran 2**.

MAKLUMAT LANJUT/KHIDMAT NASIHAT

7. Sebarang pertanyaan berkenaan Surat Pekeliling Am ini atau permohonan untuk mendapatkan khidmat nasihat berkaitan dengan pengurusan pengendalian insiden keselamatan ICT sektor awam hendaklah ditujukan kepada :

(a) Ketua Pengarah
Unit Pemodenan Tadbiran Dan Perancangan
Pengurusan Malaysia (MAMPU) ,
Aras 6, Blok B2
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA
[u.p. : *Government Computer Emergency Response Team* (GCERT)]

(b) Mel Elektronik (E-mel) : gcert@mampu.gov.my

(c) Telefon : 012-3312205

(d) Nombor Faksimili : 03-88883286

PEMAKAIAN

8. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, peruntukan Surat Pekeliling Am ini pada keseluruhannya dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Berkanun (Persekutuan dan Negeri) dan Pihak Berkuasa Tempatan.

TARIKH KUATKUASA

9. Surat Pekeliling Am ini berkuatkuasa mulai tarikh surat ini dikeluarkan.

"BERKHIDMAT UNTUK NEGARA"

(TAN SRI MOHD SIDEK HASSAN)
Ketua Setiausaha Negara