KERAJAAN MALAYSIA

PELAKSANAAN PENSIJILAN MS ISO/IEC 27001:2007 DALAM SEKTOR AWAM

JABATAN PERDANA MENTERI MALAYSIA
24 NOVEMBER 2010

Dikelilingkan kepada:

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

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

Telefon: 603 – 88723000
Faks : 603 – 88883721

Ruj. Kami : MAMPU.BPICT.700-4/3/5 Jld 2(5)
Tarikh : 24 November 2010

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

PELAKSANAAN PENSIJILAN MS ISO/IEC 27001:2007DALAM SEKTOR AWAM

TUJUAN

Surat arahan ini bertujuan untuk menjelaskan kaedah pelaksanaan dan pensijilan standard MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat (*Information Security Management System* - ISMS*)* di agensi-agensi Kerajaan.

LATAR BELAKANG

2. Mesyuarat Jemaah Menteri pada 24 Februari 2010 telah mengambil maklum bahawa tahap keselamatan maklumat kritikal negara perlu memenuhi standard antarabangsa yang boleh dicapai melalui pelaksanaan pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat.

3. Mesyuarat Jemaah Menteri juga telah bersetuju Sektor Awam yang merupakan sebahagian dari Prasarana Maklumat Kritikal Negara (*Critical National Information Infrastructure* – CNII) perlu mendapatkan pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat dalam tempoh 3 tahun. Sebarang usaha untuk mendapatkan pensijilan tersebut dalam tempoh lebih awal adalah digalakkan.

4. Bagi tujuan ini, maksud Prasarana Maklumat Kritikal Negara adalah seperti yang ditakrif di bawah Dasar Keselamatan Siber Nasional yang merangkumi aset, sistem dan fungsi ICT yang amat penting kepada Negara di mana sekiranya

keupayaan beroperasi seperti biasa terganggu akan mengakibatkan kerugian besar dari segi:

a) Kekuatan ekonomi Negara;

b) Imej nasional;

c) Pertahanan dan keselamatan;

d) Keupayaan Kerajaan berfungsi; dan

e) Kesihatan awam.

5. Dalam pada itu, agensi awam yang di luar golongan Prasarana Maklumat Kritikal Negara adalah juga digalakkan untuk turut serta mencapai pensijilan bagi menjamin kepentingan sistem penyampaian perkhidmatan pelanggan.

PELAKSANAAN

6. Dalam melaksanakan keputusan ini, Ketua Jabatan hendaklah mengambil tindakan berikut:

a) Mengatur rancangan pematuhan pensijilan ISMS sebagaimana yang telah ditetapkan oleh Jemaah Menteri dan memberi maklum balas mengikut keperluan dari masa ke masa;

b) Mengenal pasti skop pelaksanaan dan pensijilan ISMS berdasarkan perkhidmatan kritikal agensi; dan

c) Merujuk kepada dokumen-dokumen berikut sebagai panduan pelaksanaan:

i) Malaysian Standard (MS ISO/IEC 27001:2007 *Information technology - Security techniques - Information Security Management Systems – Requirement);*

ii) International Standard (ISO/IEC 27003:2009 *Information technology - Security techniques - Information Security Management System Implementation Guidance); dan*

iii) International Standard (ISO/IEC 27004: 2009 *Information Technology-Security Techniques - Information Security Management Measurement).*

KHIDMAT NASIHAT

7. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) Jabatan Perdana Menteri menyediakan khidmat rundingan ISMS dalam lima (5) bidang khusus iaitu penentuan skop ISMS agensi, penggubalan dasar keselamatan ICT agensi, melaksanakan penilaian risiko, penyediaan pelan penguraian risiko (*Risk Treatment Plan*) serta pernyataan pemakaian (*Statement of Applicability*).

8. Sebarang pertanyaan berkaitan dengan surat arahan ini dan skop pelaksanaan pensijilan ISMS hendaklah dirujuk kepada:

Ketua Pengarah
Unit Pemodenan Tadbiran dan
Perancangan Pengurusan Malaysia (MAMPU)
Jabatan Perdana Menteri
Aras 6, Blok B2, Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya

KEPERLUAN TAMBAHAN AUDIT ISMS

9. Proses audit dan pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat hendaklah dilaksanakan oleh badan pensijilan tempatan yang bertauliah dan telah diakreditasikan oleh Jabatan Standard Malaysia. Juru audit pensijilan hendaklah terdiri dari rakyat Malaysia dan mesti menandatangani Perakuan berkenaan Akta Rahsia Rasmi 1972.

PEMAKAIAN

10. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, surat arahan ini pada keseluruhannya dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Berkanun dan Pihak Berkuasa Tempatan.

KUAT KUASA

11. Surat arahan ini berkuatkuasa mula tarikh ia dikeluarkan.

"BERKHIDMAT UNTUK NEGARA"

(**DATO' MOHAMAD ZABIDI ZAINAL**)
Ketua Pengarah
Unit Pemodenan Tadbiran dan
Perancangan Pengurusan Malaysia (MAMPU)