KERAJAAN MALAYSIA

Pekeliling Am Bil.1 Tahun 2001

MEKANISME PELAPORAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

Jabatan Perdana Menteri
Malaysia
04 April 2001

Dikelilingkan Kepada:

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

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

Telefon: 603-88881957
Kawat: PERDANA
Fax: 603-88883721

Rujukan Kami: PM (S) 10034 Jld. 8 (96)
Tarikh: 04 April 2001

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

Pekeliling Am Bil.1 Tahun 2001

MEKANISME PELAPORAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

Tujuan

Pekeliling ini bertujuan untuk menjelaskan mekanisme pelaporan insiden keselamatan teknologi maklumat dan komunikasi (ICT) bagi sektor awam.

Latar Belakang

2. Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan yang dikeluarkan pada 1 Oktober 2000 melalui Pekeliling Am Bil. 3 Tahun 2000 telah merumuskan keperluan penguatkuasaan, kawalan dan langkah-langkah yang menyeluruh untuk melindungi aset ICT kerajaan bagi menjamin kesinambungan urusan kerajaan dengan meminimumkan kesan insiden keselamatan. Dengan itu satu mekanisme perlu diwujudkan untuk memantau perkara ini dan menentukan semua agensi sektor awam mematuhi dasar dan tatacara keselamatan ICT dan pada masa yang sama meningkatkan kesedaran mengenai keselamatan ICT di sektor awam.

INSIDEN KESELAMATAN

3. Insiden keselamatan bermaksud musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi (ICT) atau ancaman kemungkinan berlaku kejadian tersebut.

Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT samada yang ditetapkan secara tersurat atau tersirat.

4. Kejadian insiden boleh berlaku dalam pelbagai keadaan. Insiden yang ketara dan sering berlaku di masa kini termasuk kejadian-kejadian berikut:

(a) Percubaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran (*probing*);

(b) Serangan kod jahat (*malicious code*) seperti *virus*, *trojan horse*, *worms* dan sebagainya;

(c) Gangguan yang disengajakan (*unwanted disruption*) atau halangan pemberian perkhidmatan (*denial of service*);

(d) Menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran (*unauthorised access*); dan

(e) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.

5. Semua insiden keselamatan ICT yang berlaku di mana-mana agensi perlu dilaporkan kepada *Government Computer Emergency Response Team* (GCERT), satu pasukan khas yang ditempatkan di MAMPU bertanggungjawab menangani semua aduan mengenai insiden yang dilaporkan. Semua maklumat adalah SULIT, dengan itu tidak boleh didedahkan tanpa kebenaran agensi berkenaan.

TUJUAN PELAPORAN

6. Laporan mengenai insiden keselamatan ini adalah penting kepada GCERT untuk mendapat maklumat bagi membolehkannya menyediakan bantuan teknikal kepada agensi-agensi yang terlibat. Maklumat yang terkumpul juga boleh dijadikan panduan dalam menangani insiden yang sama yang berlaku di lokasi-lokasi yang lain. Ia juga boleh digunakan sebagai panduan bagi mengelak daripada kejadian yang sama berulang. Semua laporan yang diterima oleh GCERT akan dikumpulkan dalam pangkalan data dan maklumat ini merupakan input penting kepada perancangan strategik dan pemantauan mengenai keselamatan ICT di sektor awam. Dalam proses menyelesaikan sesuatu masalah, GCERT akan bekerjasama rapat dengan agensi terlibat dan pihak-pihak lain yang berkaitan. Interaksi seperti ini akan dapat meningkatkan pengetahuan di samping memupuk kerjasama dan hubungan baik di antara agensi.

TANGGUNGJAWAB GOVERNMENT COMPUTER EMERGENCY RESPONSE TEAM (GCERT)

7. *Government Computer Emergency Response Team* (GCERT) di MAMPU adalah bertanggungjawab menangani semua laporan insiden keselamatan ICT yang melibatkan sektor awam. Secara amnya tugas GCERT adalah seperti berikut:

(a) Menerima dan mengambil tindakan ke atas insiden keselamatan yang dilaporkan;

(b) Menyebarkan maklumat bagi membantu pengukuhan keselamatan ICT sektor awam dari semasa ke semasa;

(c) Menyediakan khidmat nasihat kepada agensi-agensi dalam mengesan, mengenalpasti dan menangani sesuatu insiden keselamatan; dan

(d) Menjadi penyelaras dengan pihak-pihak yang terlibat seperti *Malaysian Computer Emergency Response Team* (MyCERT), pembekal, *Internet Service Provider* (ISP) dan agensi-agensi penguatkuasa.

KEUTAMAAN TINDAKAN

8. Tindakan ke atas insiden yang dilaporkan akan dibuat berasaskan keparahan sesuatu insiden. Secara amnya keutamaan akan ditentukan seperti berikut:

Keutamaan 1 :
Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara.

Keutamaan 2 :
(a) Pencerobohan atau percubaan menceroboh melalui infrastruktur internet ke atas:
i. *Domain Name Servers* (DNS)
ii.*Network Access Points* (NAPs)
iii.Pusat-pusat pangkalan data utama

(b) Halangan pemberian perkhidmatan yang meluas (*Distributed Denial of Service*);

(c) Serangan atau pendedahan bahaya terbaru (*new vulnerabilities*); atau

(d) Jenis-jenis insiden lain seperti:
i. Pencerobohan melalui pemalsuan identiti
ii. Pengubahsuaian laman web, perisian, atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan pihak yang berkenaan; atau
iii. Gangguan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran.

TANGGUNGJAWAB AGENSI PELAPOR

9. Agensi yang mengalami insiden keselamatan adalah dimestikan melapor setiap insiden kepada GCERT. Setiap agensi perlu menyediakan prosidur operasi atau *Standard Operating Procedure* (SOP) berdasarkan infrastruktur ICT masing-masing supaya setiap insiden yang berlaku dapat ditangani dengan segera dan sistematik. Tugas-tugas ini diletakkan di bawah tanggungjawab Ketua Pegawai Makumat (*Chief Information Officer* - CIO) dan Pegawai Keselamatan ICT (*ICT Security Officer* - ICTSO).

10. Tugas CIO dalam aspek ini adalah seperti berikut:

(a) Menguruskan tindakan ke atas insiden yang berlaku sehingga keadaan pulih;
(b) Mengaktifkan *Business Resumption Plan* (BRP) jika perlu; dan
(c) Menentukan samada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang/keselamatan.

11. Secara khusus tugas ICTSO dalam menangani insiden keselamatan ICT pula adalah seperti berikut:

(a) Menentukan tahap keutamaan insiden;
(b) Melaporkan insiden kepada GCERT; dan
(c) Mengambil langkah pemulihan awal.

PROSES PELAPORAN

12. Proses pelaporan dijelaskan di lampiran A. Lampiran A1 menunjukkan hubungan antara agensi dan entiti yang terlibat dalam proses pelaporan manakala Lampiran A2 merupakan aliran kerja terperinci bagi proses pelaporan insiden keselamatan ICT sektor awam.

KAEDAH PELAPORAN

13. Laporan boleh dibuat menggunakan kaedah-kaedah berikut:

(a) Mel Elektronik (E-mel) :-
Alamat e-mel : mailto:gcert@mampu.gov.my

(b) Borang Pelaporan Insiden :-
Boleh diperolehi di laman : http://gcert.mampu.gov.my/

(c) Telefon Hotline
Nombor tel. : 03-88883150

(d) Faks
Nombor faksimili : 03-88883286

(e) Bagi agensi yang mempunyai kemudahan aplikasi PGP (*Pretty Good Practice*) sila gunakan PGP *Public Key* seperti di bawah untuk *encrypt* laporan yang akan dihantar kepada GCERT. Key tersebut juga boleh didapati di laman web GCERT:- http://gcert.mampu.gov.my

KHIDMAT NASIHAT

14. Sebarang kemusykilan yang timbul berkaitan dengan Surat Pekeliling ini hendaklah dirujuk kepada GCERT, seperti di bawah:

Government Computer Emergency Response Team (GCERT)
Bahagian Keselamatan ICT, MAMPU

Aras 5, Blok B1,
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA

No. Hotline : 03-88883150
No. Faksimili : 03-88883286
E-mel : gcert@mampu.gov.my

15. Khidmat GCERT boleh diperolehi setiap hari bekerja mulai pukul 8.15 pagi hingga 4.45 petang. Sekiranya agensi menghadapi insiden yang kritikal, iaitu insiden di bawah Keutamaan 1, di perenggan 8, GCERT boleh dihubungi serta merta dan jika ia berlaku di luar masa pejabat, pegawai yang boleh dihubungi adalah seperti berikut:

(a) **Bahagian Keselamatan ICT**

(i) Pengarah : 03-88882250
(ii) Timbalan Pengarah : 03-88882581

(b) **Pasukan GCERT**

(i) Pengurus : 03-88882273
(ii) Pegawai : 03-88882587

TARIKH KUATKUASA

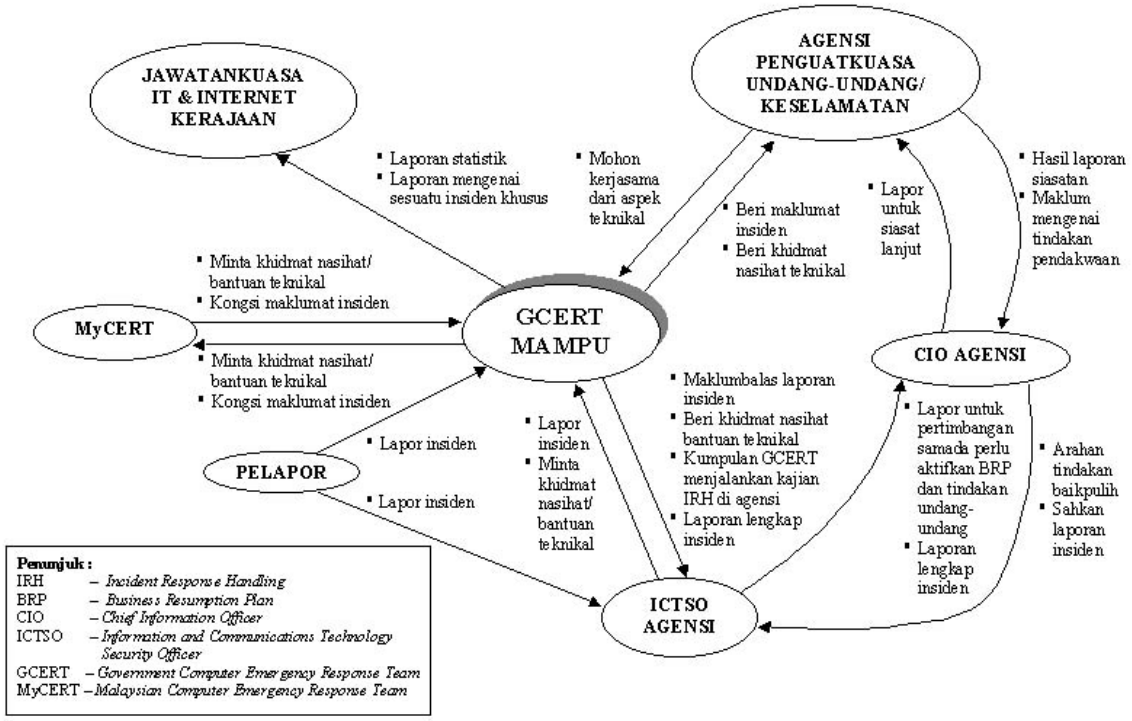
16. Surat arahan ini berkuatkuasa mulai tarikh surat ini dikeluarkan.

(TAN SRI SAMSUDIN BIN OSMAN)
Ketua Setiausaha Negara

LAMPIRAN A1

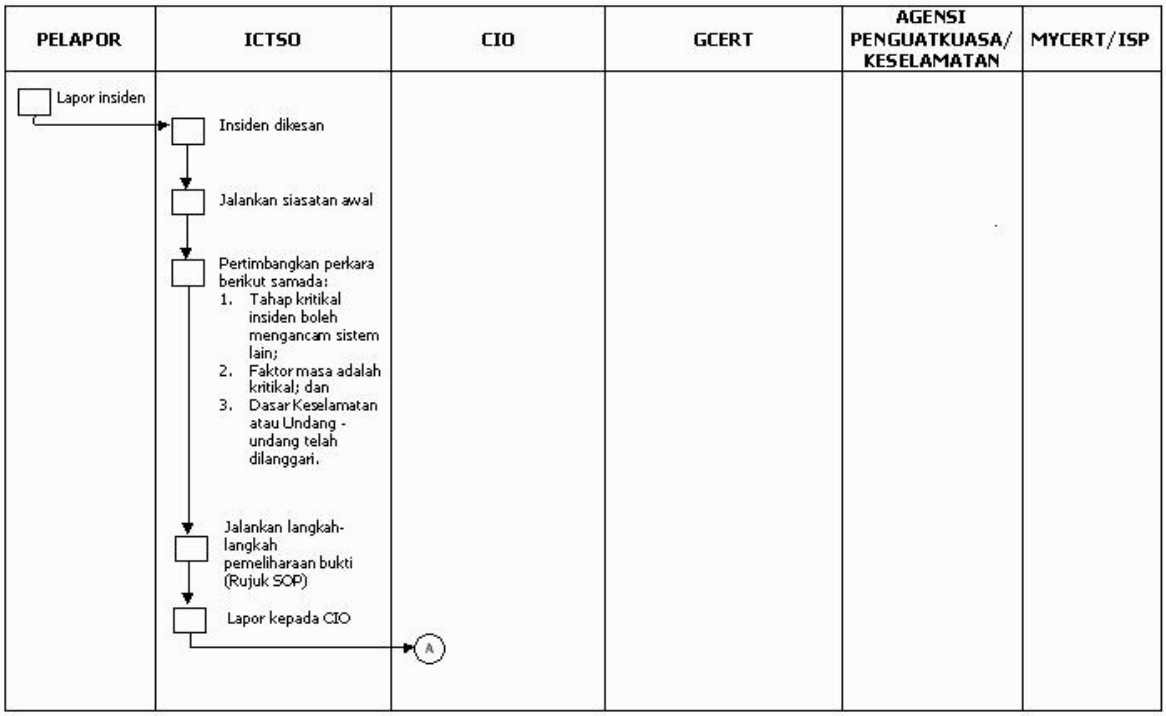
HUBUNGAN ENTITI DALAM PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT

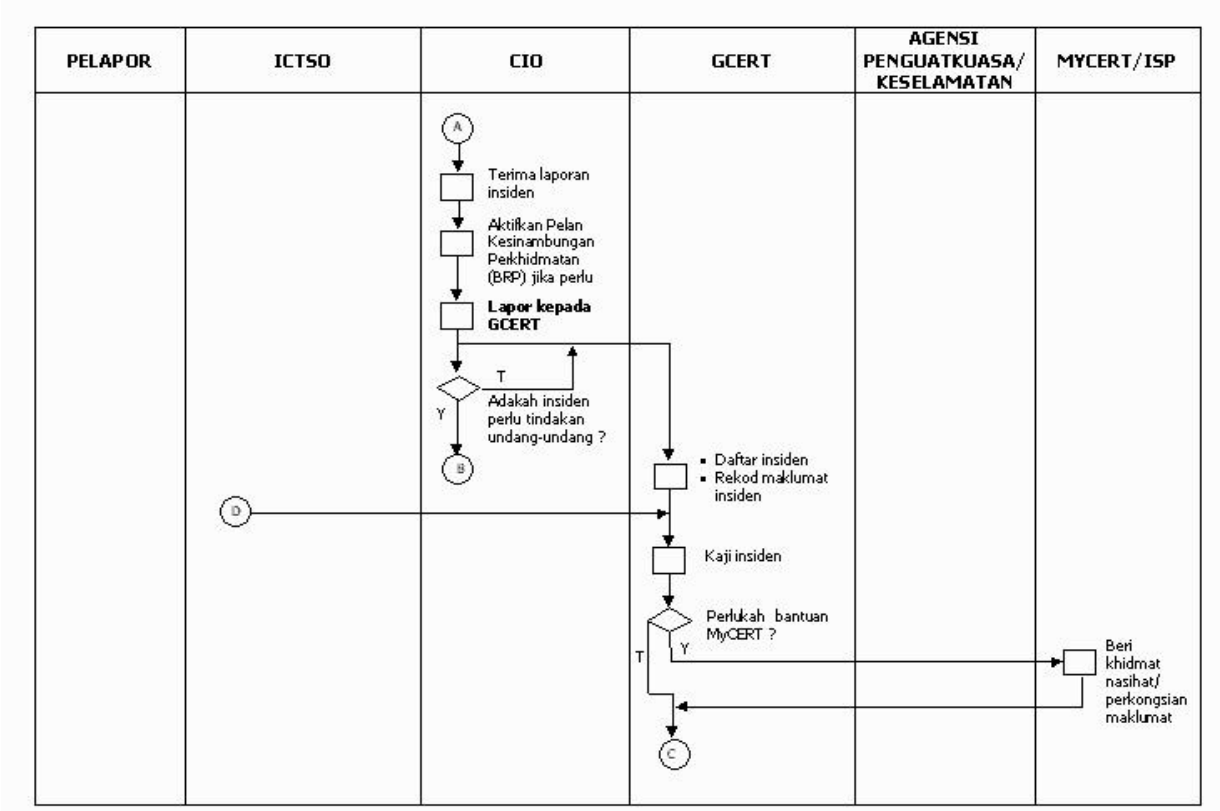
Hubungan Entiti dalam Proses Kerja Pelaporan Insiden Keselamatan ICT

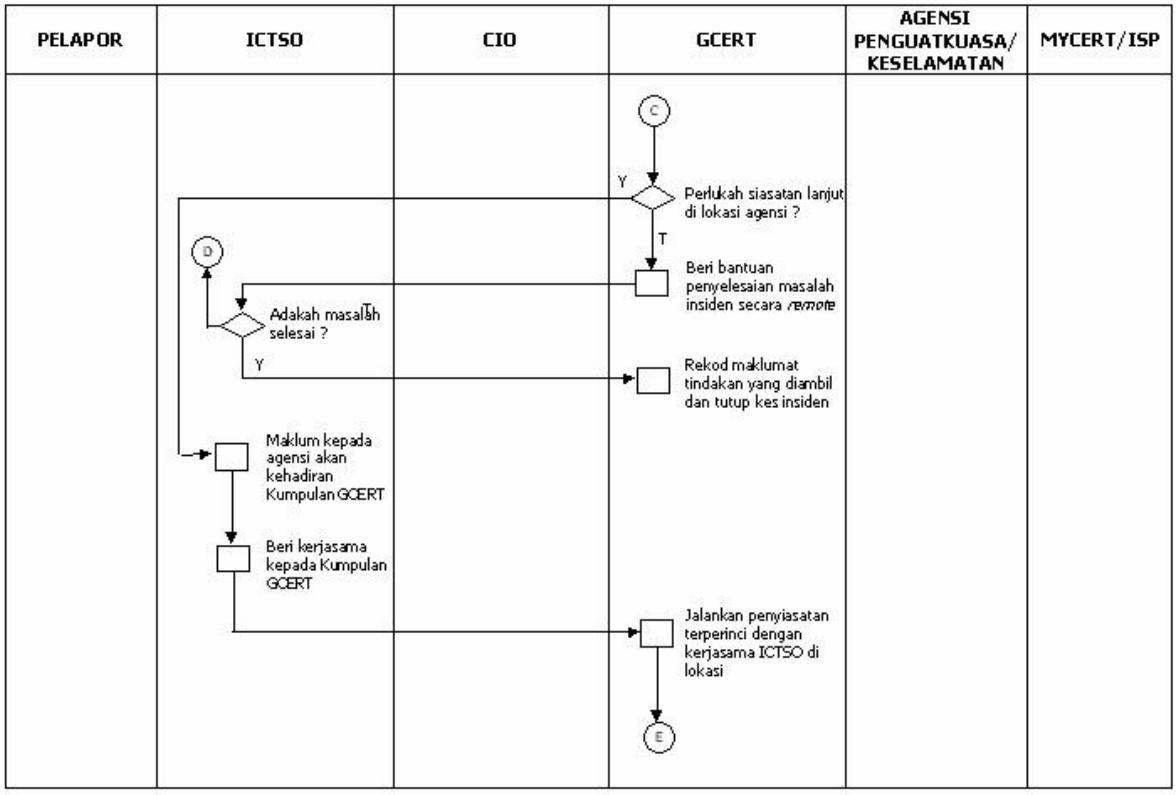


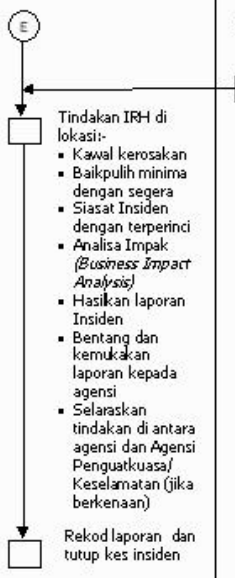
LAMPIRAN A2

JADUAL TERPERINCI BAGI PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT AGENSI YANG TERLIBAT




PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ISP
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada GCERT
T
Y
Adakah insiden perlu tindakan undang-undang ?
B
D
Daftar insiden
Rekod maklumat insiden
Kaji insiden
Perlukah bantuan MyCERT ?
Y
T
Beri khidmat nasihat/ perkongsian maklumat
C


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ISP
C
Y
Perlukah siasatan lanjut di lokasi agensi ?
T
D
Beri bantuan penyelesaian masalah insiden secara *remote*
Adakah masalah selesai ?
Y
Rekod maklumat tindakan yang diambil dan tutup kes insiden
Maklum kepada agensi akan kehadiran Kumpulan GCERT
Beri kerjasama kepada Kumpulan GCERT
Jalankan penyiasatan terperinci dengan kerjasama ICTSO di lokasi
E

PELAPOR	ICTSO	CIO	GCERT	AGENSI PENGUATKUASA/ KESELAMATAN	MYCERT/ISP
					

Nota :

SOP = *Standard Operating Procedure* yang disediakan oleh agensi