(Lampiran 1 kepada
Surat Pekeliling Am
Bilangan 4 Tahun 2006)

GARIS PANDUAN
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT SEKTOR AWAM

Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)
Jabatan Perdana Menteri

KANDUNGAN **MUKA SURAT**

GARIS PANDUAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT SEKTOR AWAM

TUJUAN

1. Tujuan garis panduan ini ialah untuk membantu *Computer Emergency Response Team* (CERT) Agensi di dalam mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.

LATAR BELAKANG

2. Kerajaan telah mengeluarkan Pekeliling Am Bilangan 1 Tahun 2001 Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) yang berkuatkuasa pada 4 April 2001 bagi menangani insiden serangan siber. Mekanisme pengurusan insiden keselamatan ICT ini adalah lebih berbentuk terpusat di mana agensi sektor awam yang mengalami insiden mesti melaporkan insiden kepada GCERT MAMPU. Memandangkan serangan siber berpotensi memberi implikasi keselamatan ke atas aset ICT dan maklumat kerajaan, usaha menangani serangan siber ke atas infrastruktur ICT sektor awam perlu ditangani dengan bijak bagi memastikan sistem ICT dapat beroperasi dengan baik tanpa gangguan.

3. Surat Pekeliling Am Bilangan 4 Tahun 2006 : Pengurusan Pengendalian Insiden Keselamatan ICT Sektor Awam menggariskan keperluan menguruskan pengendalian insiden keselamatan ICT sektor awam dengan segera dan sistematik supaya kejadian insiden keselamatan ICT di agensi sektor awam dapat dikurangkan, kesannya diminimumkan dan penyebarannya ke agensi lain dibendung.

INSIDEN KESELAMATAN ICT

4. Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT samada yang ditetapkan secara tersurat atau tersirat. Jenis insiden dapat dikenalpasti seperti berikut :

(a) **Pelanggaran Dasar (*Violation of Policy*)**

Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Dasar Keselamatan ICT.

(b) **Penghalangan Penyampaian Perkhidmatan (*Denial of Service*)**

Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal. Termasuk *denial of service* (DoS), *distributed denial of service* (DDoS) dan *sabotage*.

(c) **Pencerobohan (*Intrusion*)**

Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (*system tampering*), pindaan data (*modification of data*) dan pindaan kepada konfigurasi sistem.

(d) **Pemalsuan (*Forgery*)**

Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*) dan penipuan (*hoaxes*).

(e) ***Spam***

Spam adalah emel yang dihantar ke akaun emel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang-kali (kandungan emel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.

(f) ***Malicious Code***

Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.

(g) ***Harrassment/Threats***

Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu.

(h) ***Attempts/Hack Threats/Information Gathering***

Percubaaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran. Termasuk *spoofing, phishing, probing, war driving* dan *scanning.*

(i) **Kehilangan Fizikal (*Physical Loss*)**

Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.

TAHAP KEUTAMAAN TINDAKAN KE ATAS INSIDEN

5. Tindakan ke atas insiden yang berlaku hendaklah dibuat berasaskan kepada keparahan sesuatu insiden. Tahap keutamaan tindakan ke atas insiden akan ditentukan seperti berikut :

(a) Keutamaan 1 (Merah) – insiden keselamatan ICT yang membawa ancaman nyawa, menggugat keselamatan dan pertahanan negara, menjejas ekonomi dan imej negara, yang mungkin memerlukan Pelan Pemulihan Perkhidmatan (BCP) diaktifkan.

(b) Keutamaan 2 (Kuning) – insiden keselamatan ICT selainnya seperti pencerobohan laman web, gangguan sistem dan pencerobohan aset ICT.

PENUBUHAN CERT AGENSI

6. Sebagai langkah memperkukuhkan pengurusan pengendalian insiden ICT, semua agensi kritikal hendaklah menubuhkan CERT Agensi masing-masing. CERT Agensi bertindak sebagai *first level support* kepada GCERT MAMPU dalam mengendali insiden keselamatan ICT, mengawasi dan memberi khidmat nasihat berkaitan keselamatan ICT kepada agensi-agensi di bawah kawalannya.

7. Tiga (3) model struktur CERT Agensi adalah dicadangkan seperti berikut :

a) Model 1

Menerusi model ini, satu pasukan pengendali insiden ditubuhkan dan bertanggungjawab mengenai pengurusan insiden di agensi-agensi atau bahagian di bawah kawalannya. Model 1 digunapakai untuk kementerian, pentadbiran di peringkat negeri, institusi pengajian tinggi dan badan-badan berkanun.

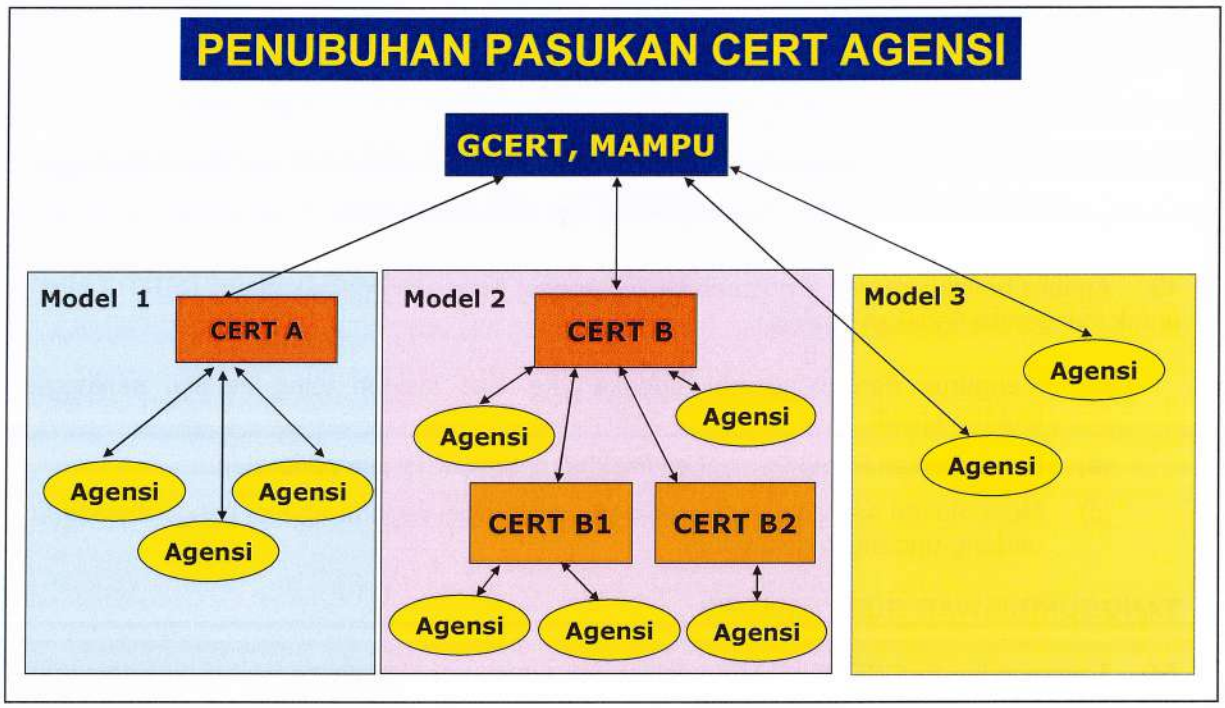
b) Model 2

Menerusi model 2, beberapa pasukan pengurus insiden ditubuhkan di peringkat jabatan atau agensi. Pasukan-pasukan ini kemudian diselaraskan di peringkat pusat CERT yang ditubuhkan di peringkat kementerian.

c) Model 3

Model ini terpakai kepada agensi-agensi yang kecil yang tidak mempunyai anggota teknikal yang mencukupi untuk mengendali dan mengurus insiden. Bagi agensi-agensi ini, sebarang insiden boleh dilaporkan terus kepada GCERT MAMPU dan pengurusan insiden keselamatan ICT akan dikendalikan oleh GCERT MAMPU.

8. Cadangan struktur ketiga-tiga model adalah dicadangkan seperti dalam **Rajah 1 : Struktur Model CERT Agensi.**



Rajah 1 : Struktur Model CERT Agensi

9. Keahlian CERT Agensi yang dicadangkan adalah seperti berikut :

(a)	Pengarah CERT	:	Ketua Pegawai Maklumat (CIO)/Pengurus Komputer
(b)	Pengurus CERT	:	Pegawai Keselamatan ICT (ICTSO)
(c)	Ahli	:	Pegawai Sistem Maklumat/ Penolong Pegawai Sistem Maklumat.

10. Keahlian CERT Agensi boleh dilantik dari kalangan anggota sedia ada yang mengendalikan operasi komputer. Bagi agensi-agensi yang mempunyai banyak pusat komputer, keahlian boleh dilantik mewakili pelbagai pusat ICT ini.

TANGGUNGJAWAB KETUA JABATAN

11. Ketua Jabatan hendaklah memainkan peranan penting bagi memastikan agensi-agensi mematuhi arahan mengenai pengurusan insiden di agensi di bawah kawalan masing-masing. Ketua Jabatan juga hendaklah memastikan kementerian, jabatan dan agensi di bawah kawalannya meningkatkan pematuhan ke atas kehendak akta, arahan, peraturan dan prosedur berkaitan keselamatan ICT.

TANGGUNGJAWAB CERT AGENSI

12. Tanggungjawab CERT Agensi meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan ICT yang dialami oleh agensi di bawah kawalannya seperti berikut :

(a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;

(b) Merekod dan menjalankan siasatan awal insiden yang diterima;

(c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baikpulih minima;

(d) Menghubungi dan melapor insiden yang berlaku kepada GCERT MAMPU samada sebagai input atau untuk tindakan seterusnya;

(e) Menasihat agensi-agensi di bawah kawalannya mengambil tindakan pemulihan dan pengukuhan;

(f) Menyebarkan makluman berkaitan insiden kepada agensi di bawah kawalannya; dan

(g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.

13. Apabila berlaku insiden, Pengarah CERT Agensi perlu menggerakkan ahli CERT Agensi untuk mengambil tindakan berikut :

(a) Mengurus dan mengambil tindakan ke atas insiden yang berlaku sehingga keadaan pulih;

(b) Mengaktifkan Pelan Pemulihan Perkhidmatan (BCP) jika perlu; dan

(c) Menentukan samada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang/keselamatan.

TANGGUNGJAWAB GCERT MAMPU

14. Tanggungjawab GCERT MAMPU dalam pengurusan pengendalian insiden keselamatan ICT sektor awam adalah seperti berikut :

(a) Menyelaras pengurusan pengendalian insiden di peringkat agensi atau antara agensi serta menasihat agensi mengambil tindakan pemulihan dan pengukuhan;

(b) Mengambil tindakan proaktif atau pencegahan seperti menjalankan imbasan keselamatan ke atas infrastruktur ICT agensi dan menyebar maklumat mengenai ancaman baru dari masa ke semasa;

(c) Menyediakan khidmat nasihat kepada CERT Agensi berkaitan dengan pengurusan dan pengedalian insiden keselamatan ICT; dan

(d) Menyelaras program pertukaran dan perkongsian maklumat antara CERT Agensi, *Malaysian Computer Emergency Response Team* (MyCERT), pembekal, *Internet Service Provider* (ISP) dan agensi-agensi penguatkuasa.

15. GCERT MAMPU juga bertanggungjawab kepada agensi-agensi kecil (struktur CERT Model 3) dalam mengurus pengendalian insiden keselamatan ICT seperti berikut :

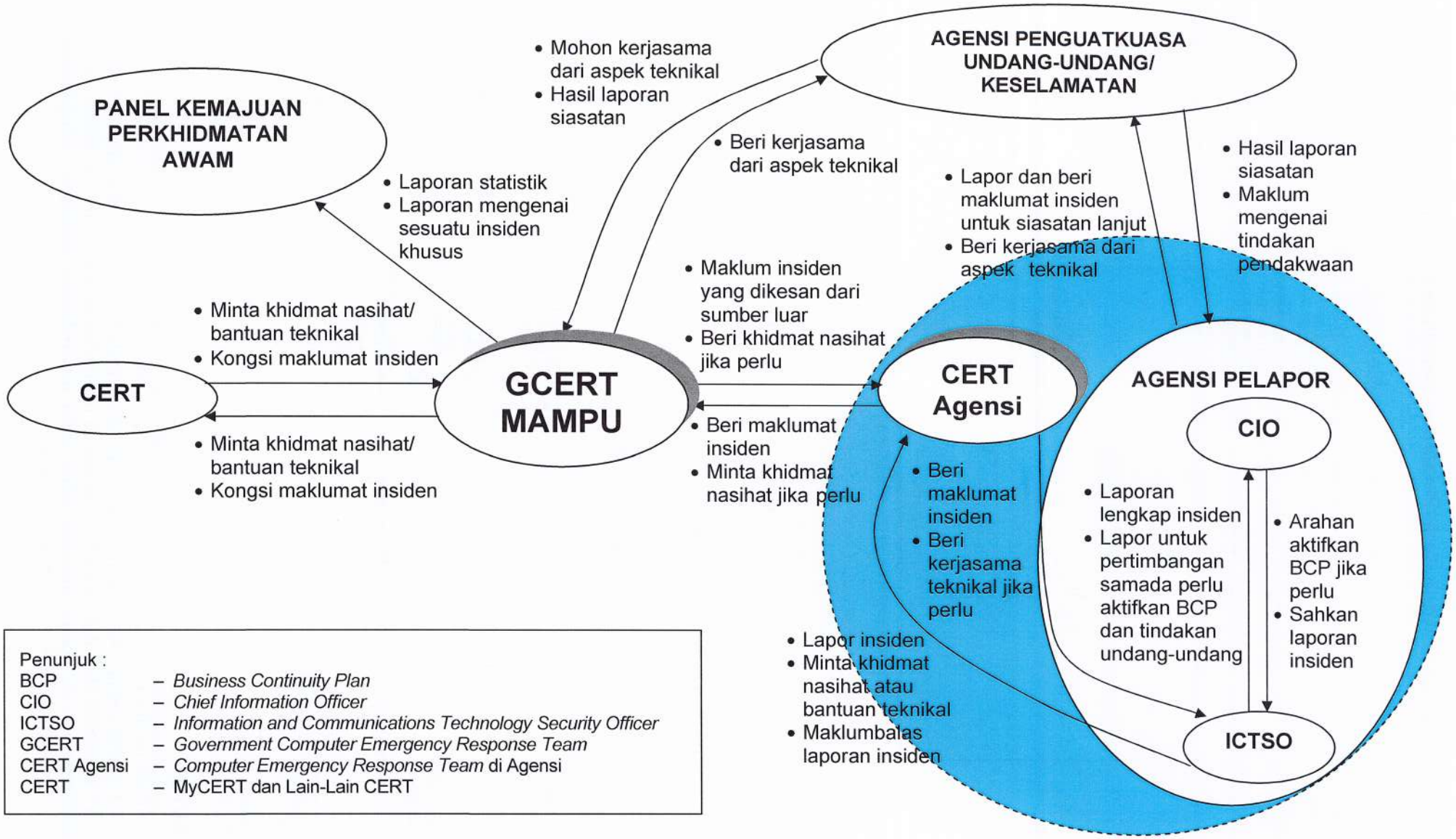
(a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; dan

(b) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengemukakan cadangan tindakan baikpulih minima.

PROSES PELAPORAN INSIDEN KESELAMATAN ICT SEKTOR AWAM

16. Proses Pelaporan Insiden Keselamatan ICT Sektor Awam diringkaskan dalam **Rajah 2 – Hubungan Entiti Dalam Proses Kerja Pelaporan Insiden Keselamatan ICT** dan **Rajah 3 – Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT** di bawah. Proses pengendalian insiden keselamatan ICT diterangkan secara terperinci dalam Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamtan ICT CERT Agensi.

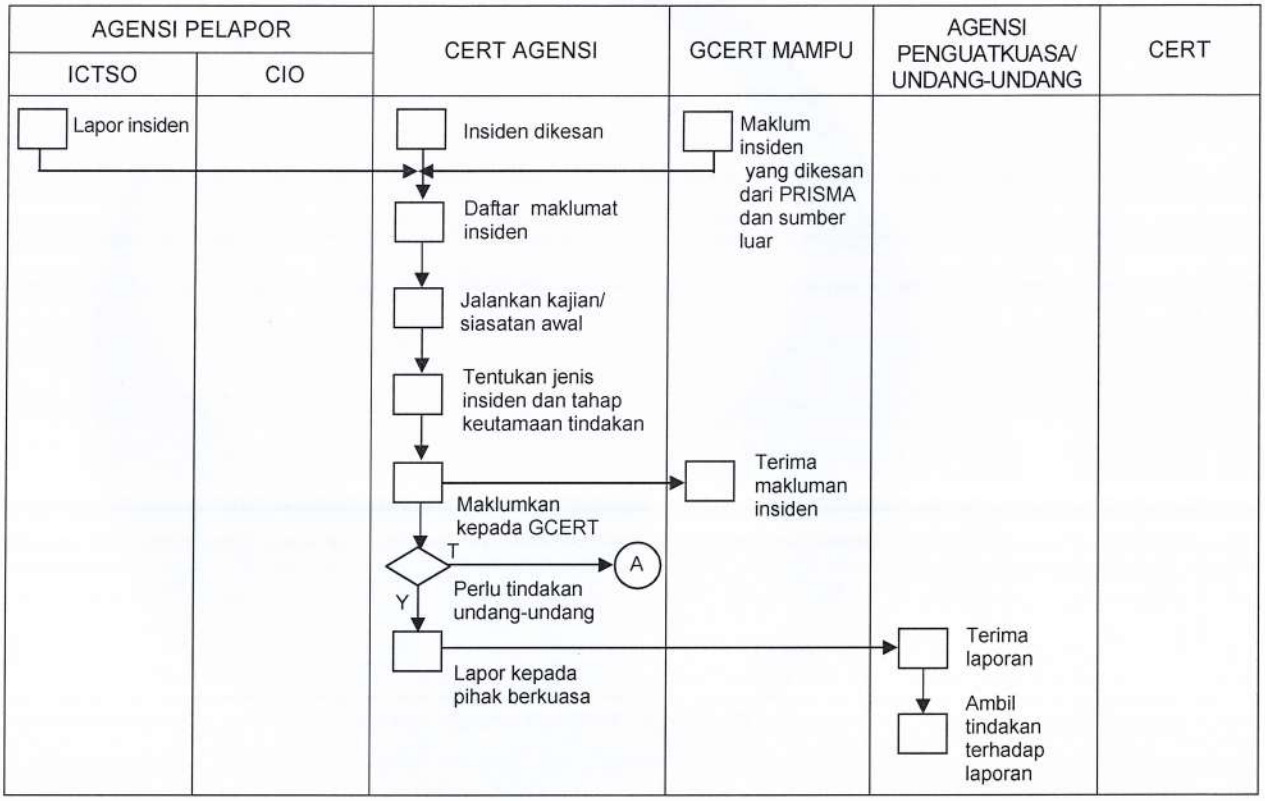
Rajah 2 : Hubungan Entiti Dalam Proses Kerja Pengurusan Pelaporan Insiden Keselamatan ICT

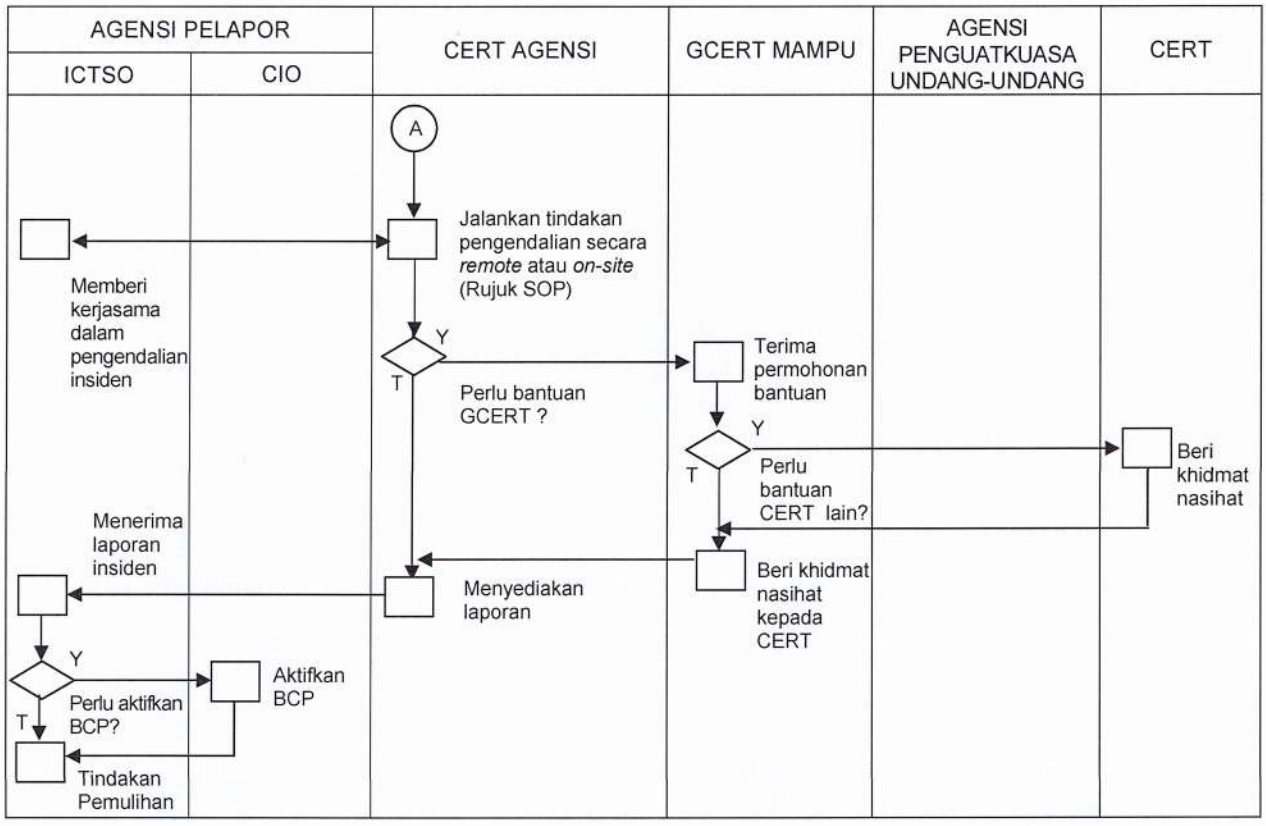


Penunjuk :

BCP	– *Business Continuity Plan*
CIO	– *Chief Information Officer*
ICTSO	– *Information and Communications Technology Security Officer*
GCERT	– *Government Computer Emergency Response Team*
CERT Agensi	– *Computer Emergency Response Team* di Agensi
CERT	– MyCERT dan Lain-Lain CERT

Rajah 3 : Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT Agensi





PENUTUP

17. Garis panduan ini disediakan untuk membantu *Computer Emergency Response Team* (CERT) Agensi memperkemaskan pengurusan pengendalian insiden keselamatan ICT sektor awam bagi memperkasakan agensi sektor awam menguruskan sendiri pengendalian insiden keselamatan ICT di agensi masing-masing serta meningkatkan kecekapan pengendalian insiden keselamatan ICT di agensi sektor awam.