KERAJAAN MALAYSIA

SURAT PEKELILING AM BIL. 4 TAHUN 2006

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

JABATAN PERDANA MENTERI
MALAYSIA

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 : 603-88881957
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 Pihak Berkuasa Badan Berkanun
Semua Pihak Berkuasa Tempatan

SURAT PEKELILING AM BIL. 4 TAHUN 2006

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

TUJUAN

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

LATAR BELAKANG

2. Kerajaan telah mengeluarkan Pekeliling Am Bil. 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 diperjelaskan di mana usaha menangani serangan siber ke atas infrastruktur ICT kerajaan perlu ditangani dengan bijak bagi mempastikan 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 dan Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT Sektor Awam. 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 Agensi Pelapor;
(g) Tanggungjawab GCERT MAMPU; dan
(h) Proses Pelaporan Insiden Keselamatan ICT Sektor Awam

6. Prosedur Operasi Standard pula mengandungi proses terperinci dalam pengendalian insiden keselamatan ICT iaitu:

(a) Template Borang IRH 1.0 : Laporan Pengendalian Insiden;
(b) Template Borang IRH 1.1 : Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT;
(c) Panduan Komunikasi Pengendalian Insiden Secara Jarak Jauh; dan
(d) Template Laporan Analisa Log.

Garis Panduan Pengurusan Pengendalian Insiden Keselamatan ICT dan Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT Sektor Awam 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) , Jabatan Perdana Menteri,
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

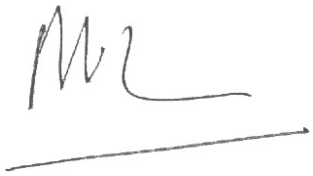
PEMAKAIAN

13. 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

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

"BERKHIDMAT UNTUK NEGARA"



(TAN SRI MOHD SIDEK HASSAN)
Ketua Setiausaha Negara

(Lampiran 1 kepada
Surat Pekeliling Am
Bil. 4 Tahun 2006)

KERAJAAN MALAYSIA

GARIS PANDUAN
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT SEKTOR AWAM

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

6 NOVEMBER 2006

KANDUNGAN **MUKA SURAT**

1.	Tujuan	3
2.	Latar Belakang	3
3.	Insiden Keselamatan ICT	3
4.	Tahap Keutamaan Tindakan ke atas Insiden	4
5.	Penubuhan CERT Agensi	5
6.	Tanggungjawab Ketua Jabatan	6
7.	Tanggungjawab CERT Agensi	7
8.	Tanggungjawab GCERT MAMPU	7
9.	Proses Pelaporan Insiden Keselamatan ICT Sektor Awam	8
10.	Penutup	12

GARIS PANDUAN
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

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 Bil. 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 mempastikan sistem ICT dapat beroperasi dengan baik tanpa gangguan.

3. Surat Pekeliling Am Bil. 4 Tahun 2006 : Garis Panduan 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*), 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 akan 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.

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 *Business Resumption Planning* diaktifkan.

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

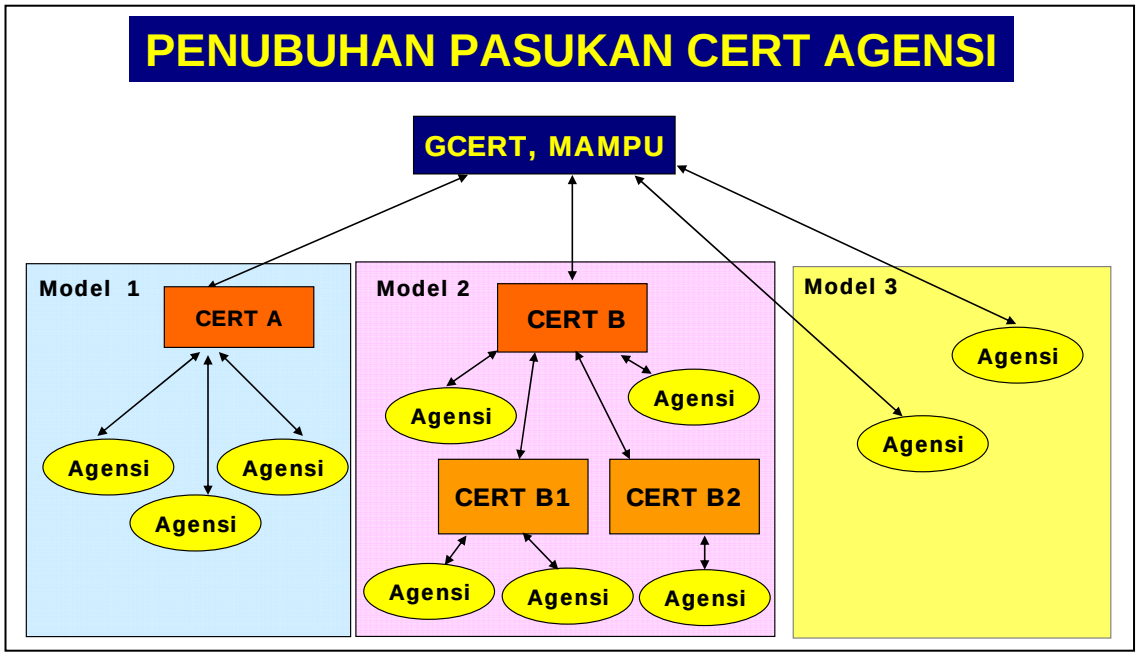
b) Model 2

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, pengurusan insiden keselamaan ICT akan dikendalikan oleh GCERT MAMPU dan mereka boleh terus melapor sebarang insiden kepada 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 mempastikan agensi-agensi mematuhi arahan mengenai pengurusan insiden di agensi di bawah kawalan masing-masing. Ketua Jabatan juga hendaklah mempastikan kementerian, jabatan dan agensi di bawah kawalannya meningkatkan pematuhan ke atas kehendak akta, arahan, peraturan dan prosidur 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; dan

(f) menyebarkan makluman berkaitan dengan agensi di bawah kawalannya; dan

(g) Menjalankan penilaian untuk mempastikan 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 Kesinambungan Perkhidmatan (BRP) 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;

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

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

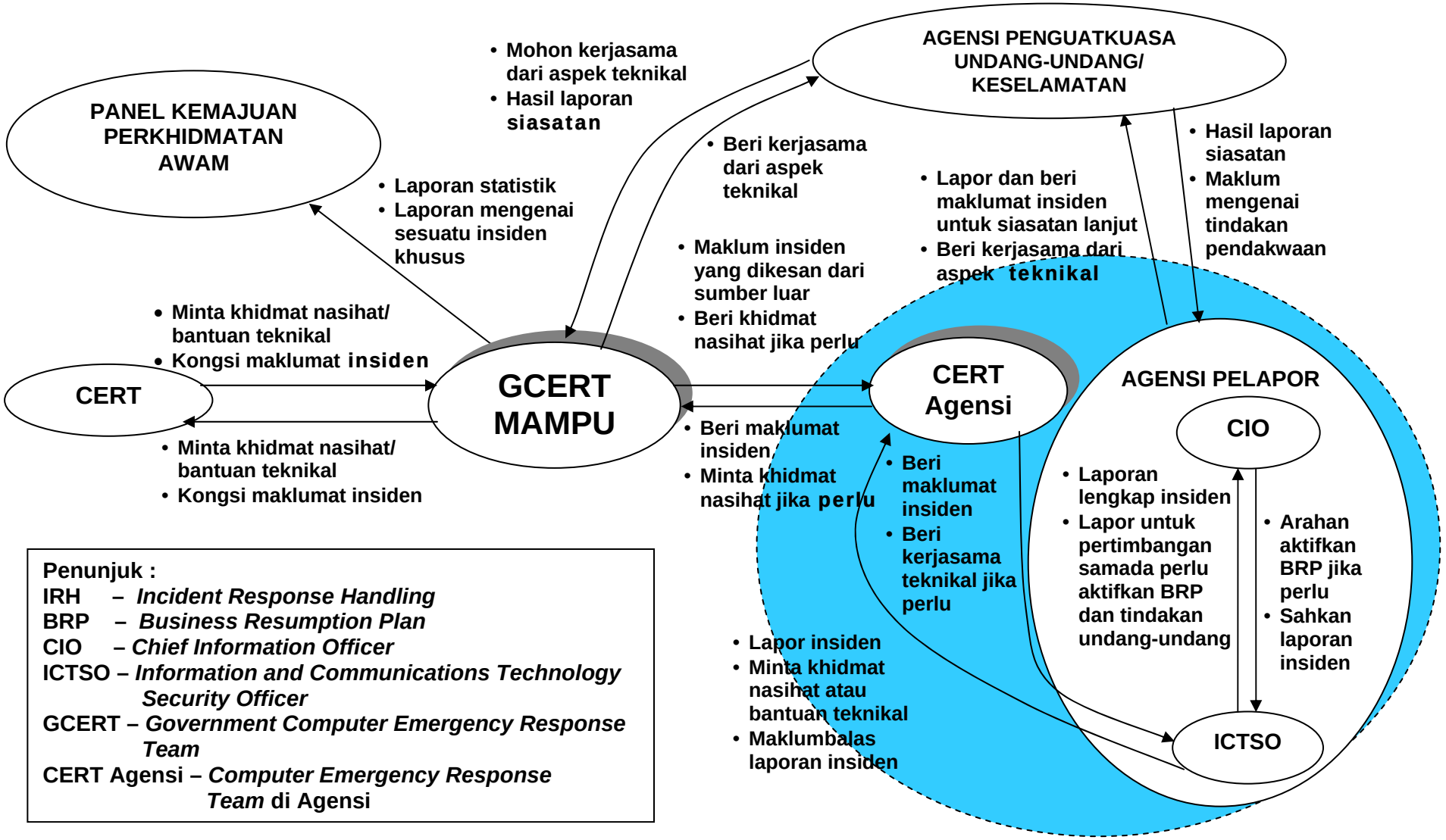
(a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; dan

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

PROSES PELAPORAN INSIDEN KESELAMATAN ICT SEKTOR AWAM

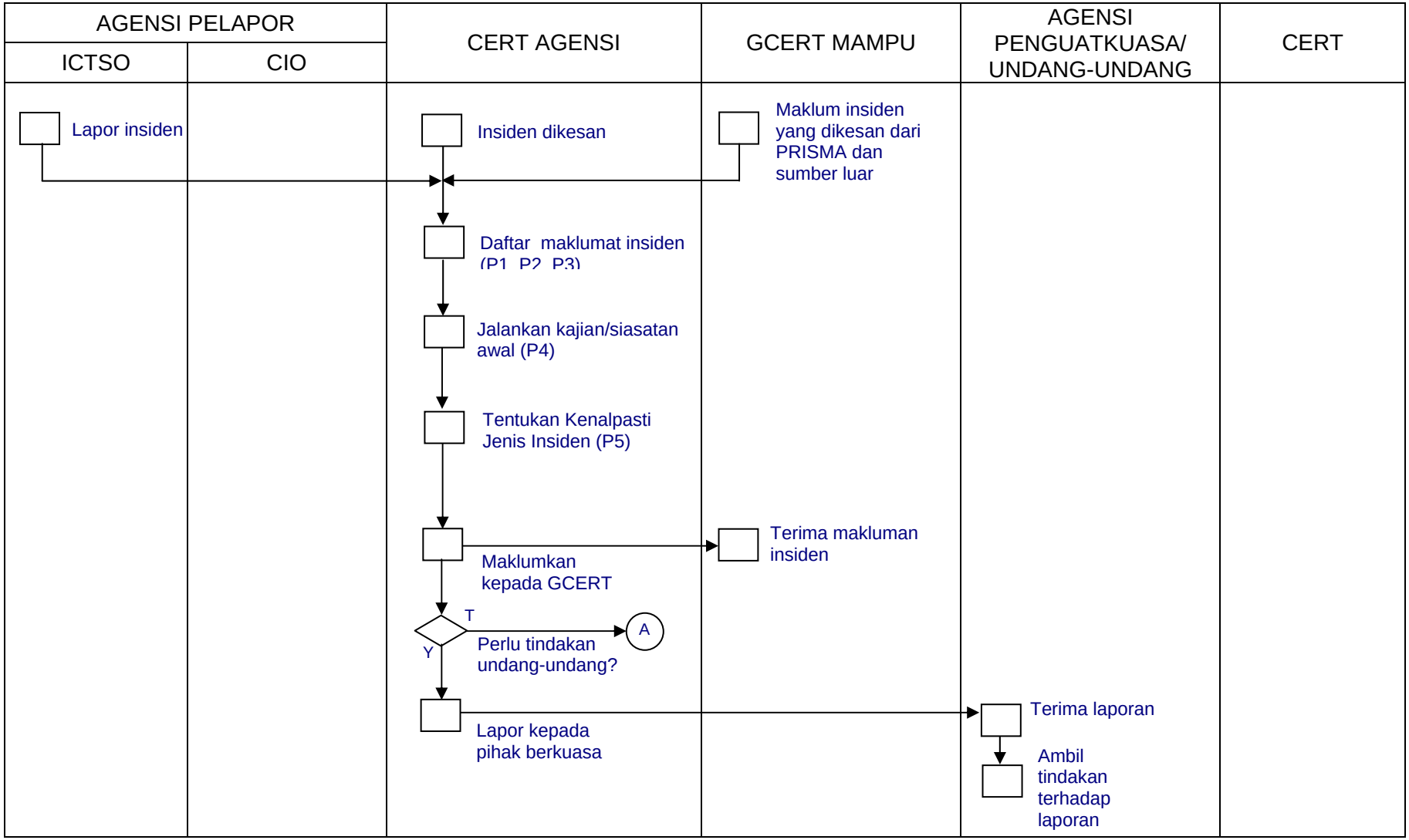
16. Proses Pelaporan Insiden Keselamatan ICT Sektor Awam diringkaskan dalam **Rajah 2 – Hubungan Entiti Dalam Proses Kerja Pelaporan Insiden Keselamatan ICT** dan **Rajah 3 – Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT** di bawah. Proses pengendalian insiden keselamatan ICT diterangkan secara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

Rajah 1 : Hubungan Entiti Dalam Proses Kerja Pengurusan Pelaporan Insiden Keselamatan ICT

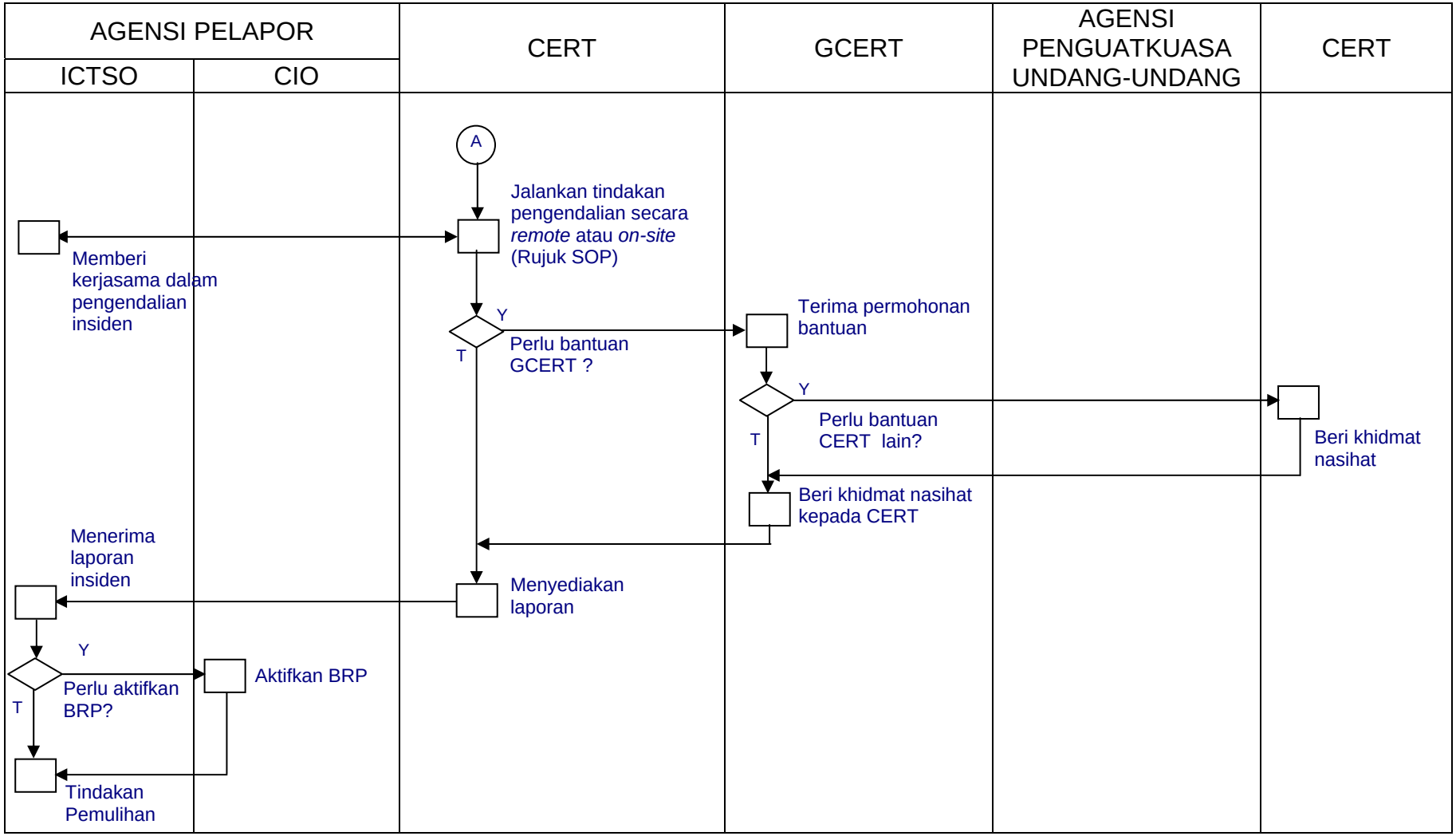


Penunjuk :
IRH – *Incident Response Handling*
BRP – *Business Resumption Plan*
CIO – *Chief Information Officer*
ICTSO – *Information and Communications Technology Security Officer*
GCERT – *Government Computer Emergency Response Team*
CERT Agensi – *Computer Emergency Response Team* di Agensi

Rajah 2 : Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT Agensi



Rajah 2 : 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 keselamatan ICT di agensi sektor awam.

(Lampiran 2 kepada
Surat Pekeliling Am
Bil. 4 Tahun 2006)

KERAJAAN MALAYSIA

PROSEDUR OPERASI STANDARD PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT SEKTOR AWAM

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

6 NOVEMBER 2006

KANDUNGAN **MUKA SURAT**

1. OBJEKTIF 3

2. PROSEDUR OPERASI STANDARD 3

- Pentadbiran *Incident Response Handling* (IRH) 4
- Pengurusan Pengendalian Insiden 5
- Pengendalian Insiden Secara Jarak Jauh (*Remote*) 7
- Pengendalian Insiden Di Lokasi Agensi Terlibat (*On site*) 12
- Penyebaran Maklumat 24
- Penyelarasan Pengurusan Insiden Keselamatan ICT 28

3. LAMPIRAN

- Template Borang IRH 1.0 : Laporan Pengendalian Insiden 29
- Template Borang IRH 1.1 : Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT oleh Agensi 31
- Panduan Komunikasi Pengendalian Insiden 32
- Template Laporan Analisis Log 41
- Singkatan Perkataan 42

PROSEDUR OPERASI STANDARD PENGENDALIAN INSIDEN KESELAMATAN ICT CERT AGENSI

OBJEKTIF

1. Dokumen ini menerangkan prosedur yang digunapakai oleh CERT Agensi bagi mengendalikan insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.

PROSEDUR OPERASI STANDARD

2. Secara amnya, tanggungjawab CERT Agensi adalah meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan ICT yang dialaminya dan yang dialami oleh agensi di bawah kawalannya:

(a) **Pentadbiran (*Administration*)**

Bidang pentadbiran merangkumi tugas-tugas merekod aduan, mengemaskini maklumat insiden dan menyelenggara fail data insiden untuk membantu kelancaran operasi CERT Agensi.

(b) Pengendalian Insiden (*Incident Response Handling* – IRH)

Tugas-tugas pengendalian insiden dijalankan apabila aduan di terima dari agensi di bawah kawalan sehingga kes insiden selesai dikendalikan. Bidang tugas ini meliputi proses-proses penerimaan laporan insiden, penyiasatan kes, penyediaan laporan selepas pengendalian serta khidmat nasihat kepada agensi terlibat.

(c) **Penyebaran Maklumat**

Setiap CERT Agensi mestilah menyebarkan maklumat berkaitan insiden keselamatan ICT dari semasa ke semasa kepada agensi-agensi di bawah kawalannya dan GCERT MAMPU bagi berkongsi maklumat untuk meningkatkan tahap keselamatan ICT agensi dan membendung insiden keselamatan ICT sektor awam. Penyebaran maklumat ini dilaksanakan secara reaktif dan proaktif. Penyebaran maklumat dilakukan secara reaktif bagi insiden yang telah berlaku dan secara proaktif mengenai *vulnerabilities* dan ancaman yang bakal melanda agensi supaya tindakan pengukuhan dilakukan untuk mengelakkan kejadian insiden ke atas agensi di bawah kawalannya.

(d) **Penyelarasan Pengurusan Pengendalian Insiden**

CERT Agensi berperanan menyelaraskan mesyuarat pengurusan pengendalian insiden keselamatan ICT di antara

agensi-agensi di bawah kawalannya dan pihak-pihak lain yang terlibat dalam pengendalian insiden keselamatan ICT. Agenda utama mesyuarat adalah untuk berkongsi maklumat bagi meningkatkan tahap keselamatan ICT dan membendung kejadian insiden keselamatan ICT di antara agensi-agensi di bawah kawalannya dan sektor awam amnya.

3. **Pentadbiran *Incident Response Handling* (IRH)**

(a) Terima dan rekod insiden dari agensi di bawah kawalan

(b) Tadbir dan selenggara fail-fail/pangkalan data insiden

(c) Kemaskini maklumat insiden selepas siasatan

Proses 1 - Terima Dan Rekod Insiden Dari Agensi Di Bawah Kawalan

Tugas 1.1 - Mencatat maklumat awal insiden

Keterangan Aktiviti	Mekanisme /Rujukan	Tindakan
1. Setiap aduan yang diterima perlu dicatatkan dalam borang, buku log/fail atau pangkalan data berkaitan.	• Buku / fail / sistem Log • Borang IRH 1.0 – Laporan Pengendalian Insiden	• Pegawai CERT Agensi

Proses 2 - Tadbir Dan Selenggara Fail-Fail/Pangkalan Data Insiden

Tugas 2.1 - Mentadbir dan menyelenggara fail-fail insiden

Keterangan Aktiviti	Mekanisme /Rujukan	Tindakan
1. Sekiranya catatan dibuat ke dalam borang, failkan borang berkenaan dan kemaskini rekod statistik insiden.	• Borang IRH 1.0 – Laporan Pengendalian Insiden • Statistik insiden • Surat • E-mail • Faks • Fail Sulit	• Pegawai CERT Agensi
2. Simpan maklumat/ dokumen yang berkaitan ke dalam server dengan mengambil kira perkara-perkara berikut: a) *Encrypt* maklumat /dokumen insiden; dan	• Fail Server CERT Agensi	• Pegawai CERT Agensi

Keterangan Aktiviti	Mekanisme /Rujukan	Tindakan
b) Dokumen disimpan mengikut nama direktori agensi masing-masing (CERT Fail Server/ nama_agensi/no_ insiden-nama_pegawai)		

Proses 3 - Kemaskini Maklumat Insiden Selepas Siasatan

Tugas 3.1 - Mengemaskini maklumat insiden selepas siasatan

Keterangan Aktiviti	Mekanisme /Rujukan	Tindakan
1. Kemaskini maklumat insiden yang diperolehi semasa siasatan ke dalam fail-fail / pangkalan data insiden.	• Fail Server/Media CERT Agensi	• Pegawai CERT Agensi

4. Pengurusan Pengendalian Insiden

(a) Jalankan kajian atau siasatan awal ke atas insiden

(b) Tentukan jenis dan tahap keutamaan tindakan ke atas insiden

(c) Agihkan tugas dan kaedah pengendalian insiden

(d) Beri khidmat bantuan dari segi teknikal kaedah menangani insiden secara jarak jauh (*remote*) atau di lokasi (*onsite*)

(e) Sediakan laporan lengkap

Proses 4 - Jalankan Kajian Atau Siasatan Awal Insiden

Tugas 4.1 - Menjalankan kajian atau siasatan awal ke atas insiden

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Dapatkan maklumat tambahan mengenai insiden dengan berpandukan soalan-soalan dan langkah-langkah yang perlu dilakukan oleh pegawai yang dihubungi di agensi.	• Panduan Komunikasi Pengendalian Insiden Secara Jarak Jauh	• 2 hari	• Pegawai CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
2. Menyemak laman web yang menyenaraikan insiden pencerobohan ke atas laman web kerajaan Malaysia.	• Rujuk laman web: http://www.zone-h.org	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi • Pegawai CERT Agensi

Proses 5 - Tentukan Jenis Dan Tahap Keutamaan Tindakan ke atas Insiden

Tugas 5.1 - Menentukan jenis insiden dan tahap keutamaan tindakan ke atas insiden

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Berdasarkan kajian dan siasatan awal ke atas insiden, tentukan jenis kes dan kesan kerosakan ke atas agensi di bawah kawalan.	• Panduan Komunikasi Pengendalian Insiden Secara Jarak Jauh	• 2 hari	• Pegawai CERT Agensi
2. Berikan nasihat awal dan dapatkan fail log terlibat.		• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi
3. Maklum dan berbincang dengan Pengurus CERT Agensi untuk agihan tugas pengendalian dan penentuan tahap severity insiden.		• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi • Pegawai CERT Agensi
4. Maklumkan insiden kepada GCERT MAMPU.		• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi • Pegawai CERT Agensi

Proses 6 - Agihkan Tugas Dan Kaedah Pengendalian Insiden

Tugas 6.1 - Mengagihkan tugas pengendalian insiden

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Semak status pengendalian insiden semasa.	• Fail atau pangkalan data pengurusan pengendalian insiden	• 2 hari	• Pengurus CERT Agensi
2. Agihkan tugas dan kaedah pengendalian insiden kepada pegawai CERT Agensi.		• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi • Pegawai CERT Agensi

5. Pengendalian Insiden Secara Jarak Jauh (*Remote*)

(a) Jalankan siasatan lanjut secara jarak jauh (*remote*)

(b) Sediakan laporan analisis fail-fail log

(c) Pengesahan terhadap laporan analisis fail log

(d) Kemukakan laporan analisis fail-fail log kepada agensi

(e) Pelaksanaan imbasan Hos

(f) Tindakan Pemulihan

(g) Penutupan kes insiden

(h) Kemaskini maklumat dan status insiden

Proses 7 - Jalankan Siasatan Lanjut Secara Jarak Jauh (*Remote*)

Tugas 7.1 - Susul dengan pegawai yang dihubungi di agensi terlibat

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Hubungi pegawai berkaitan di agensi terlibat.	• Borang IRH 1.0 - Laporan Pengendalian Insiden	• 2 hari	• Pegawai CERT Agensi
2. Dapatkan fail-fail log berkaitan dan beri tunjuk ajar kepada pegawai di agensi	• Borang IRH 1.0 - Laporan Pengendalian Insiden	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
langkah-langkah untuk mendapatkan fail log berkenaan.			
3. Analisis fail-fail log yang diterima.		• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi

Proses 8 - Sediakan Laporan Analisis Fail-Fail Log

Tugas 8.1 - Menyediakan laporan analisis fail-fail log

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Berdasarkan fail-fail log yang diterima dan analisis ke atas fail-fail log tersebut, sediakan laporan analisis log beserta nasihat serta cadangan tindakan pengukuhan. (Dapatkan bantuan GCERT sekiranya perlu)	• Fail-fail log diperolehi dari agensi • Template laporan analisis log	• 2 hari	• Pegawai CERT Agensi

Proses 9 - Pengesahan Terhadap Laporan Analisis Fail Log

Tugas 9.1 - Semak dan beri maklumbalas terhadap laporan analisis fail log

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Laporan analisis berserta nasihat cadangan tindakan pengukuhan disemak dan pengesahan atau maklumbalas diberikan.	• Fail-Fail Log Diperolehi Dari Agensi • Laporan Analisis Fail Log	• 2 hari	• Pengurus CERT Agensi

Proses 10 - Kemukakan Laporan Analisis Fail-Fail Log Kepada Agensi

Tugas 10.1 - Mengemukakan laporan analisis fail-fail log kepada agensi terlibat

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Laporan analisis berserta nasihat cadangan tindakan pengukuhan disemak dan makluman mengenai pelaksanaan imbasan hos selepas lima hari dari tarikh penerimaan laporan.	• Laporan Analisis Fail Log • Cadangan Tindakan Pengukuhan • Makluman Mengenai Pelaksanaan Imbasan Hos	• 2 hari	• Pegawai CERT Agensi

Proses 11 - Pelaksanaan Imbasan Hos

Tugas 11.1 - Melaksanakan imbasan hos dan menyediakan laporan analisis imbasan hos

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Laksanakan imbasan hos ke atas server agensi terlibat.		• 2 hari	• Pegawai CERT Agensi
2. Jalankan analisis ke atas laporan imbasan hos ke atas server agensi terlibat.		• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi
3. Sediakan laporan analisis imbasan hos dan kemukakan untuk semakan dan pengesahan.		• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi

Tugas 11.2 - Menyemak dan mengesahkan laporan analisis imbasan hos

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Semak dan sahkan atau beri malumbalas mengenai laporan analisis imbasan hos.		• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi
2. Sediakan laporan analisis imbasan hos dan kemukakan untuk semakan dan pengesahan.			• Pegawai CERT Agensi

Tugas 11.3 - Kemukakan laporan analisa imbasan hos kepada agensi terlibat

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Kemukakan laporan analisis imbasan hos kepada agensi dan minta agensi kembalikan borang IRH 1.1 selepas 5 hari laporan diterima oleh agensi.		• 2 hari	• Pegawai CERT Agensi

Proses 12 - Tindakan pemulihan

Tugas 12.1 - Tindakan pemulihan oleh agensi pelapor

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Laksanakan tindakan pemulihan berdasarkan laporan analisis imbasan hos.		• 5 hari	• Agensi Pelapor

Tugas 12.2 - Tindakan pemantauan pemulihan ke atas agensi pelapor

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Memantau pelaksanaan tindakan pemulihan oleh agensi pelapor berdasarkan laporan analisis imbasan hos.		• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi

Proses 13 - Penutupan Kes Insiden

Tugas 13.1 - Penutupan Kes Insiden

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pantau penerimaan borang IRH 1.1		• 2 hari	• Pegawai CERT Agensi
2. Sekiranya maklumbalas diterima dari IRH 1.1 menyatakan bahawa tindakan pengukuhan telah dilaksanakan, pohon kebenaran menutup kes insiden.		• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi
3. Beri kebenaran kes untuk ditutup, sekiranya Pengurus CERT Agensi berpuashati dengan maklumbalas diterima.		• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi
4. Maklumkan kepada GCERT mengenai penutupan kes.		• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi • Pengurus CERT Agensi

Proses 14 - Kemaskini Maklumat Dan Status Insiden

Tugas 14.1 - Mengemaskini Maklumat Dan Status Insiden

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Kemaskini maklumat dan status pengendalian insiden ke dalam fail atau pangkalan data insiden.	• Fail / Pangkalan Data Insiden • Statistik Insiden	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi

6. Pengendalian Insiden Di Lokasi (On site)

(a) Jalankan siasatan lanjut di lokasi (*on-site*)

(b) Mesyuarat pengurusan IRH di agensi

(c) Siasatan terperinci *Incident Response Handling (IRH)*

(d) Penyediaan laporan awal pentadbiran CERT Agensi

(e) Penyediaan laporan insiden

(f) Cetakan laporan akhir insiden

(g) Kemukakan laporan akhir yang disahkan kepada agensi

(h) Penutupan kes

Proses 15 - Jalankan Siasatan Lanjut Di Lokasi (*On-Site*)

Tugas 15.1 - Hubungi agensi untuk dapatkan maklumat lanjut dan membuat temu janji dengan agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pegawai CERT Agensi menghubungi agensi terlibat untuk mendapatkan: a) maklumat lanjut b) memberi nasihat awal		• 2 hari (* Tempoh pengendalian bergantung sama ada agensi berjaya/gagal dihubungi)	• Pegawai CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
2. Mendapatkan persetujuan daripada agensi pelapor (ICTSO/ Pengurus Komputer) bagi CERT Agensi menjalankan siasatan lanjut di lokasi dan membuat temu janji bagi mengadakan mesyuarat IRH. Maklumat yang diperlukan adalah tarikh, masa dan tempat temu janji.	• Borang IRH 1.0 - Laporan Pengendalian Insiden	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi
3. Pegawai CERT Agensi memaklumkan kepada Pengurus CERT Agensi sekiranya agensi tidak bersetuju untuk mengadakan mesyuarat pengurusan IRH bagi menjalankan siasatan lanjut di lokasi (*On-site*) secara lisan atau e-mel.	• Borang IRH 1.0 - Laporan Pengendalian Insiden	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi
4. Pengurus CERT Agensi memaklumkan kepada Pengarah CERT Agensi secara lisan atau e-mel bahawa CERT Agensi akan menjalankan siasatan lanjut di lokasi (*on-site*).	• Borang IRH 1.0 - Laporan Pengendalian Insiden	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi
5. Mendapatkan kebenaran untuk keluar stesen jika perlu.	• Borang Keluar Stesen	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi

Tugas 15.2 - Sediakan kelengkapan pengendalian insiden

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pegawai CERT Agensi menyediakan kelengkapan seperti berikut*:* a) *Notebook;* b) Borang yang berkaitan; c) Disket/*Thumb Drive;* d) *Hard disk;* dan e) Perisian dan peralatan forensik.	• Borang IRH 1.0 - Laporan Pengendalian Insiden	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi
2. Pengurus CERT Agensi memastikan semua kelengkapan pengendalian insiden adalah mencukupi.	-	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi

Proses 16 - Mesyuarat Pengurusan IRH Di Agensi

Tugas 16.1 - Jalankan mesyuarat pengurusan IRH dengan agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Mesyuarat IRH dihadiri oleh: a) Agensi pelapor i. Ketua Jabatan / Ketua Bahagian IT ii. ICTSO iii. Pentadbir Sistem	• Borang IRH 1.0 - Laporan Pengendalian Insiden • SANS	• 1 hari	• Agensi pelapor • Pengarah CERT Agensi (sekiranya perlu) • Pengurus CERT Agensi • Pegawai CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
b) CERT Agensi i. Pengarah CERT Agensi ii. Pengurus CERT Agensi iii. Pegawai CERT Agensi c) Wakil GCERT (sekiranya perlu)			
2. Perbincangan mesyuarat meliputi: i. Tujuan IRH di lokasi (*On-site*). ii. Mendapatkan maklumat lanjut pencerobohan iii. Memaklumkan proses-proses IRH iv. Melaporkan kepada Pihak Penguatkuasa PDRM (sekiranya perlu) dan CERT Agensi akan membantu penyiasatan sekiranya diperlukan.	• Borang IRH 1.0 - Laporan Pengendalian Insiden • SANS	• 1 hari	• Agensi pelapor • Pengarah CERT Agensi (sekiranya perlu) • Pengurus CERT Agensi • Pegawai CERT Agensi
3. Pegawai CERT Agensi mencatatkan keseluruhan proses kronologi insiden keselamatan ICT bermula dari mesyuarat dijalankan sehingga proses pengendalian insiden tersebut selesai.	-	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi

Proses 17 - Siasatan Terperinci IRH

Tugas 17.1 - Jalankan siasatan terperinci ke atas infrastruktur ICT yang diceroboh

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pegawai CERT Agensi menjalankan siasatan lanjut ke atas sistem/*server* yang diceroboh (bergantung kepada keperluan) seperti berikut: a) Mendapatkan data forensik; b) Membuat 2 salinan ke *atas hard disk;* c) Menyalin fail-fail log sistem, aplikasi dan firewall; d) Mencari fail-fail hasil tinggalan penceroboh seperti *backdoor, trapdoor, trojan horse*, *virus* dan *worm;* e) Menjalankan *port scanning*; f) Memasang *packet sniffing;* g) Menjalankan *vulnerability scanning; dan* h) *File Usage Activity.*	• Perisian Dan Peralatan Forensik	• 7 hari	• Pegawai CERT Agensi • Pengurus CERT Agensi
2. Menganalisa maklumat/bukti-bukti pencerobohan yang diperolehi hasil daripada siasatan lanjut ke atas sistem/*server* yang diceroboh.	• Sumber Internet	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi • Pegawai CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
3. Memaklumkan kepada agensi pelapor secara lisan mengenai tindakan dan status siasatan sistem/*server* yang diceroboh dari semasa ke semasa serta tindakan seterusnya.	-	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi • Pegawai CERT Agensi

Tugas 17.2 - Jalankan proses baik pulih ke atas infrastruktur ICT yang diceroboh

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Menjalankan aktiviti-aktiviti seperti berikut: a) Format semula sistem/*server* yang diceroboh (jika perlu) b) *Install* semula sistem pengoperasian c) *Install* perisian anti-virus dengan *signature* terkini d) *Restore* menggunakan *backup* data	-	• 7 hari	• Agensi pelapor

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
2. Sekiranya sistem/*server* tidak perlu diformat: a) Menjalankan *backup* ke atas sistem b) Menukar kata laluan yang sedia ada kepada yang lebih selamat Contohnya: Gabungkan simbol + huruf + nombor) c) Hapuskan fail-fail hasil tinggalan penceroboh seperti *backdoor, trapdoor, trojan horse, virus* atau *worm* d) Membuat *restore* dengan menggunakan *backup* data e) *Install* atau kemas kini perisian anti-virus dengan *signature* terkini	-	• Dalam tempoh yang sama seperti di atas	• Agensi pelapor
3. Memberi khidmat nasihat kepada agensi pelapor mengenai langkah-langkah pengukuhan dan tindakan yang perlu diambil dari semasa ke semasa bagi meningkatkan tahap keselamatan ICT agensi pelapor.	-	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi • Pegawai CERT Agensi

Proses 18 - Penyediaan Laporan Awal Pentadbiran CERT Agensi

Tugas 18.1 - Sediakan deraf laporan awal pentadbiran CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pegawai CERT Agensi perlu menyediakan draf laporan awal hasil siasatan IRH di lokasi (*On-site)* untuk makluman pihak pengurusan atasan agensi di CERT Agensi (Ketua Jabatan) dan mengemukakan deraf laporan tersebut kepada Pengurus CERT Agensi bagi tujuan semakan dan pengesahan.	• Laporan Awal Siasatan CERT Agensi • Borang IRH 1.0 - Laporan Pengendalian Insiden	• 3 hari	• Pegawai CERT Agensi • Pengurus CERT Agensi

Tugas 18.2 - Pengesahan dan kelulusan deraf laporan awal pentadbiran CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pengurus CERT Agensi membuat semakan dan pengesahan draf laporan awal siasatan CERT Agensi dan mengemukakan kepada Pengarah CERT Agensi untuk kelulusan.	• Laporan Awal Siasatan CERT Agensi	• 1 hari	• Pengurus CERT Agensi • Pengarah CERT Agensi
2. Pengarah CERT Agensi mempertimbang dan meluluskan laporan awal siasatan CERT Agensi yang lengkap.	• Laporan Awal Siasatan CERT Agensi	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi • Pengarah CERT Agensi

Tugas 18.3 - Kemukakan laporan awal pentadbiran CERT Agensi kepada pihak pengurusan CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pengarah CERT Agensi kemukakan dan menerangkan secara ringkas laporan awal siasatan CERT Agensi kepada pihak pengurusan atasan agensi di CERT Agensi (Ketua Jabatan)	• Laporan Awal Siasatan CERT Agensi	• 1 hari	• Pengarah CERT Agensi

Proses 19 - Penyediaan Laporan Insiden

Tugas 19.1 - Sediakan laporan dan slaid pembentangan insiden pencerobohan

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pegawai CERT Agensi akan mengemaskini draf laporan kronologi insiden keselamatan ICT yang sedia ada, menyediakan laporan teknikal yang terperinci dan menyediakan slaid pembentangan insiden pencerobohan untuk dikemukakan kepada Pengurus CERT Agensi bagi tujuan semakan dan pengesahan.	• Borang Kronologi Insiden Keselamatan ICT • Laporan Insiden Pencerobohan Keselamatan ICT (Teknikal) • Slaid Pembentangan Insiden Pencerobohan	• 14 hari	• Pegawai CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
2. Pengurus CERT Agensi akan menyediakan draf laporan pengurusan untuk pihak Pengurusan Atasan agensi di CERT Agensi dan agensi dibawah tanggungjawab CERT Agensi hasil daripada pengumpulan maklumat insiden pencerobohan yang dijalankan.	• Laporan Insiden Pencerobohan Keselamatan ICT (Pengurusan)	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi

Tugas 19.2 - Semak deraf laporan insiden pencerobohan keselamatan ICT (Teknikal)

Keterangan	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pengurus CERT Agensi menyemak dan mengesahkan draf laporan kronologi insiden keselamatan ICT, laporan insiden pencerobohan keselamatan ICT (Teknikal) dan slaid pembentangan insiden pencerobohan sebelum dikemukakan kepada Pengarah CERT Agensi.	• Borang Kronologi Insiden Keselamatan ICT • Laporan Insiden Pencerobohan Keselamatan ICT (Teknikal) • Slaid Pembentangan Insiden Pencerobohan	• 1 hari	• Pengurus CERT Agensi

Tugas 19.3 - Kemukakan laporan insiden pencerobohan keselamatan ICT (Pengurusan dan Teknikal) dan slaid pembentangan insiden pencerobohan kepada Pengarah CERT Agensi

Keterangan	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pengurus CERT Agensi kemukakan laporan insiden pencerobohan keselamatan ICT (Pengurusan dan Teknikal) kepada Pengarah CERT Agensi untuk semakan dan pengesahan.	• Laporan Insiden Pencerobohan Keselamatan ICT (Pengurusan) • Laporan Insiden Pencerobohan Keselamatan ICT (Teknikal) • Slaid Pembentangan Insiden Pencerobohan	• 1 hari	• Pengurus CERT Agensi

Tugas 19.4 - Kelulusan laporan insiden

Keterangan	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pengarah CERT Agensi akan meluluskan laporan dan slaid pembentangan insiden pencerobohan keselamatan ICT (Pengurusan dan Teknikal) sebelum dikemukakan dan dibentangkan kepada agensi pelapor.	• Laporan Insiden Pencerobohan Keselamatan ICT (Pengurusan) • Laporan Insiden Pencerobohan Keselamatan ICT (Teknikal)	• 1 hari	• Pengarah CERT Agensi

Proses 20 - Cetakan Laporan Akhir Insiden

Tugas 20.1 - Cetak laporan akhir insiden pencerobohan keselamatan ICT

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pegawai CERT Agensi membuat cetakan laporan akhir insiden pencerobohan keselamatan ICT (Pengurusan dan Teknikal) sebanyak tiga (3) salinan kepada: a) Agensi pelapor; b) GCERT; dan c) Fail CERT Agensi.	• Laporan insiden pencerobohan keselamatan ICT (Pengurusan) • Laporan insiden pencerobohan keselamatan ICT (Teknikal)	• 1 hari	• Pegawai CERT Agensi

Proses 21 - Kemukakan Laporan Akhir Insiden Kepada Agensi Pelapor

Tugas 21.1 - Hantar laporan akhir insiden pencerobohan keselamatan ICT (*hardcopy*) kepada agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Menyediakan surat untuk dilampirkan bersama laporan insiden pencerobohan keselamatan ICT kepada agensi pelapor.	-	• 1 hari	• Pegawai CERT Agensi
2. Mengemukakan laporan insiden pencerobohan keselamatan ICT dan surat (untuk agensi pelapor) kepada Pengurus CERT Agensi untuk ditandatangani.	-	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
3. Menghantar dokumen laporan akhir insiden dengan mengikut prosidur surat SULIT.	• Buku Arahan Keselamatan	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi
4. Menghubungi agensi pelapor bagi memastikan dokumen Laporan IRH telah diterima.	-	• Dalam tempoh yang sama seperti di atas	• Pegawai CERT Agensi

Proses 22 - Penutupan Kes

Tugas 22.1 - Bentang laporan akhir insiden pencerobohan keselamatan ICT kepada agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pegawai CERT Agensi membuat temu janji bersama agensi pelapor bagi menjalankan pembentangan laporan insiden pencerobohan keselamatan ICT.	-	• 1 hari	• Pegawai CERT Agensi
2. Pengurus CERT Agensi akan membentangkan laporan insiden pencerobohan.	-	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi

Tugas 22.2 - Kemaskini statistik insiden

Keterangan	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Pegawai CERT Agensi mengemaskini statistik insiden pencerobohan untuk tujuan perekodan dan memasukkan	• Statistik Insiden • Fail Sulit	• 1 hari	• Pegawai CERT Agensi

Keterangan	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
dokumen yang berkaitan ke dalam fail SULIT.			
2. Maklumkan kepada GCERT mengenai penutupan kes.		• 1 hari	• Pegawai CERT Agensi

7. Penyebaran Maklumat

i) Mendapat maklumat dari internet atau agensi lain

ii) Kajian terperinci terhadap ancaman dan impak insiden

iii) Sediakan nota makluman mengenai ancaman

iv) Penyebaran nota makluman

Proses 23 - Mendapat Maklumat Dari Internet Atau Agensi Lain

Tugas 23.1 - Merekodkan maklumat dari internet atau aduan dari agensi.

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Dapat dan rekod aduan dari agensi.	• Buku / fail / sistem Log • Borang IRH 1.0 – Laporan Pengendalian Insiden	• 1 hari	• Pegawai CERT Agensi • Pengurus CERT Agensi

Tugas 23.2 - Mendapat maklumat dari internet atau agensi lain.

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Mendapatkan maklumat dari internet atau agensi lain.	• Sumber Internet • Borang IRH 1.0 – Laporan Pengendalian Insiden	• 1 hari	• Pegawai CERT Agensi • Pengurus CERT Agensi

Proses 24 - Kajian Terperinci Terhadap Ancaman Dan Impak Insiden

Tugas 24.1 - Menjalankan aktiviti kajian.

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Menjalankan analisa ke atas aduan atau maklumat yang diperolehi.	• Sumber Internet	• 3 hari	• Pengawai CERT Agensi
2. Mendapatkan maklumat lanjut.	• Agensi Terlibat • Sumber Internet • Sumber Lain	• Dalam tempoh yang sama seperti di atas	• Pengawai CERT Agensi
3. Memaklumkan kepada agensi mengenai status kajian dan tindakan yang perlu diambil.	• Borang IRH 1.0 – Laporan Pengendalian Insiden	• Dalam tempoh yang sama seperti di atas	• Pengawai CERT Agensi
4. Menyediakan laporan terperinci mengenai insiden/ancaman keselamatan ICT, tahap kerosakan dan impak.	• Laporan Terperinci Insiden / Ancaman	• Dalam tempoh yang sama seperti di atas	• Pengawai CERT Agensi

Proses 25 - Sediakan Nota Makluman Mengenai Ancaman

Tugas 25.1 - Sediakan deraf laporan awal kajian/penemuan

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Menyediakan deraf nota makluman dan ringkasan mengenai insiden/ancaman keselamatan ICT, tahap kerosakan dan impak.	• Nota Makluman • Laporan Terperinci Insiden / Ancaman • Laporan Ringkas	• 1 hari	• Pengawai CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
2. Membuat semakan dan pengesahan deraf nota makluman untuk dikemukakan kepada Pengarah CERT Agensi.	• Nota Makluman • Laporan Ringkas	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi
3. Mengemukakan nota makluman dan syor kaedah penyebaran makluman insiden/ancaman kepada Pengarah CERT Agensi.	• Nota Makluman • Laporan Ringkas	• Dalam tempoh yang sama seperti di atas	• Pengurus CERT Agensi
4. Membuat keputusan mengenai tindakan penyebaran.	• Nota Makluman • Laporan Ringkas	• Dalam tempoh yang sama seperti di atas	• Pengarah CERT Agensi

Proses 26 - Penyebaran Nota Makluman

Tugas 26.1 - Menyebarkan nota makluman kepada ICTSO agensi di bawah kawalan

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Menghantar e-mel kepada semua ICTSO agensi di bawah kawalan dan GCERT.	• Nota Makluman • Laporan Ringkas	• 1 hari	• Pegawai CERT Agensi

Tugas 26.2 - Kemukakan nota makluman kepada pihak pengurusan atasan agensi di CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Menyediakan deraf nota makluman dan ringkasan mengenai insiden/ancaman keselamatan ICT, tahap kerosakan	• Nota Makluman • Laporan Terperinci Insiden/Maklumat Ancaman	• 1 hari	• Pengurus CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
dan impak untuk tujuan semakan Pengarah CERT Agensi.	• Laporan Ringkas		
2. Membuat semakan dan pengesahan deraf nota makluman untuk dikemukakan kepada pihak pengurusan atasan agensi di CERT Agensi.	• Nota Makluman • Laporan Ringkas	• Dalam tempoh yang sama seperti di atas	• Pengarah CERT Agensi
3. Mengemukakan nota makluman dan syor kaedah penyebaran makluman insiden/ancaman kepada pihak pengurusan atasan agensi di CERT Agensi.	• Nota Makluman • Laporan Ringkas	• Dalam tempoh yang sama seperti di atas	• Pengarah CERT Agensi
4. Membuat keputusan mengenai tindakan penyebaran.	• Nota Makluman • Laporan Ringkas	• Dalam tempoh yang sama seperti di atas	• Pengurusan Atasan CERT Agensi

8. Penyelarasan Pengurusan Insiden Keselamatan ICT

Proses 27 - Penyelarasan Pengurusan Insiden Keselamatan ICT

Tugas 27.1 - Pengurusan mesyuarat penyelarasan insiden keselamatan ICT

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Mengadakan mesyuarat penyelarasan pengurusan keselamatan insiden ICT.	• Nota Cadangan	• 1 hari	• Pengurus CERT Agensi

TEMPLATE BORANG

Borang IRH 1.0 : Laporan Pengendalian Insiden

SULIT

Borang IRH 1.0- Laporan Pengendalian Insiden Tarikh Pengendalian :

Computer Emergency Response Team Agensi (CERT Agensi)	
*No. Insiden	Tahun/Bulan/Kod Kategori/Bil insiden dalam tahun semasa **(Diisi oleh CERT Agensi)**
*Tarikh & Masa Dikesan	**(Diisi oleh CERT Agensi)**
Maklumat Organisasi/Agensi	
ICTSO 1. Nama 2. E-mel 3. No. Telefon Pejabat 4. No. Telefon Bimbit	
Pentadbir Sistem 1. Nama 2. E-mel 3. No. Telefon Pejabat 4. No. Telefon Bimbit	
Pegawai Perhubungan 1. Nama 2. E-mel 3. No. Telefon Pejabat 4. No. Telefon Bimbit	
Alamat Penuh Agensi	
Bahagian/Unit Yang Melapor	
No. Telefon Agensi	
No. Faks	
Maklumat Perkakasan dan Perisian Yang Terlibat	
Hostname	
Domain	
DNS	
Alamat IP 1. Internal 2. External	
Sistem Pengoperasian 1. Jenis 2. Versi 3. Service pack	
Kapasiti Disk	

Jenis *Hard Disk*
Sistem Aplikasi / Perkhidmatan lain
Maklumat Insiden
Alamat IP Penyerang
Jenis Insiden e.g. unauthorized access, malicious code
Jenis Serangan
Keterangan Lanjut Mengenai Insiden (Nyatakan tarikh, masa, jenis kerosakan, kesan ke atas maklumat atau sistem dan lain-lain maklumat yang dikira relevan sekiranya diketahui.)

Tarikh dan Masa :	
Jenis Kerosakan :	
Kesan Ke Atas : Maklumat/Sistem	
Perkakasan ICT : Yang Terlibat & Bil.	
Khidmat Teknikal :	☐ Pembekal ☐ Dalaman – Bil. ..... orang Lain-Lain : .....
Kos Terlibat :	RM

Tindakan Yang Diambil Oleh Agensi
Sila penuhkan ruang ini. (Sila jelaskan dengan terperinci tindakan yang telah diambil untuk - meminimumkan risiko pencerobohan atau menghalangnya sama-sekali, - membaik pulih perkhidmatan sistem)
Tindakan Yang Diambil Oleh CERT Agensi (Diisi oleh Pegawai Cert Agensi)
(Diisi oleh CERT Agensi)

Borang IRH 1.1 : Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT oleh Agensi

Kepada:

Pengarah
Alamat CERT Agensi

Merujuk kepada Laporan *Host Scanning*/serangan siber bertarikh _____ adalah dimaklumkan tindakan pengukuhan keselamatan ICT * **TELAH/BELUM** dijalankan sebagaimana yang telah dicadangkan.

(* Potong yang tidak berkenaan dan jelaskan jika **BELUM**)

_____

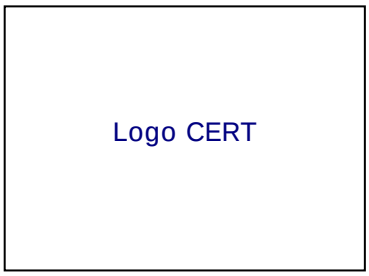
_____

Pelaksanaan Pengukuhan Oleh:

Nama:
Jawatan:
Tarikh:
Telefon:
E-mel:

Pengesahan Oleh Ketua Jabatan/Ketua Pegawai Maklumat (CIO):

Nama:
Jawatan:
Tarikh:
Telefon:
E-mel:
Alamat:



Panduan Komunikasi Pengendalian Insiden Secara Jarak Jauh

http:// (laman web ICT Security Agensi)

Alamat CERT Agensi

PERHATIAN: Sila tandakan ✓ pada ruangan OK .

Bil.	Perkara
1.0	**Pengenalan** a) Situasi 1: CERT Agensi menghubungi agensi Saya _____ (nyatakan nama Pegawai IRH) daripada CERT Agensi. Pihak CERT Agensi mendapat makluman bahawa server agensi tuan/puan telah diceroboh. CERT Agensi ingin mendapatkan maklumat terperinci mengenai server tersebut bagi membantu siasatan. Untuk makluman tuan/puan maklumat ini adalah SULIT dan mohon kerjasama pihak tuan/puan memberi keterangan lanjut mengenai insiden ini. b) Situasi 2: Agensi menghubungi CERT Agensi **Nota:** • Kedua-dua situasi perlu merujuk kepada soalan-soalan di bawah:
2.0	**Maklumat Organisasi/Agensi** a) Boleh saya dapatkan maklumat tuan/puan? i. ICTSO • Nama • E-mel • No. Telefon Pejabat • No. Telefon Bimbit ii. Pentadbir Sistem • Nama • E-mel • No. Telefon Pejabat • No. Telefon Bimbit iii. Pegawai Untuk Dihubungi • Nama • E-mel • No. Telefon Pejabat • No. Telefon Bimbit **Nota:** Telefon bimbit diperlukan supaya Pegawai bertanggungjawab mudah dihubungi di masa kecemasan atau di luar waktu pejabat

	b) Alamat Penuh Agensi i. Boleh saya dapatkan alamat lengkap agensi tuan/puan? ii. Boleh saya tahu nama Bahagian yang bertanggungjawab? iii. Boleh saya tahu agensi tuan/puan di bawah Kementerian/Jabatan mana? c) Nombor telefon agensi/Faks Boleh saya dapatkan nombor telefon agensi/faks di pejabat tuan/puan?
3.0	**Maklumat Perkakasan dan Perisian Yang Terlibat** Boleh saya dapatkan beberapa maklumat mengenai server yang diceroboh? a) *Hostname* (nama server) b) Domain (jika berkaitan dengan *website*) c) DNS d) Alamat IP (*Internal/External*) e) Alamat MAC (jika berkaitan) Cara untuk mendapatkan Alamat IP dan MAC adalah seperti berikut: **i. Win NT/Win 2000/Win 2003** • ***Klik Start > Run > Taip cmd*** • ***Skrin DOS akan memaparkan prompt c:/> Taip ipconfig /all*** **ii. Linux/Unix/BSD** • ***Buka terminal*** • ***Taip ifconfig -a*** f) Sistem Pengoperasian • Jenis • Versi • *Service Pack*

Cara untuk mendapatkan maklumat sistem pengoperasian adalah seperti berikut:

i. Win NT/Win 2000/Win 2003

- Jenis
- Versi
- *Service Pack*

* **Nota**

Cara 1:

Klik Start > Setting >

Control Panel > System

Cara 2:

Lihat pada http:// www.netcraft.com yang mana laman web tersebut menyatakan maklumat OS yang dicari

ii. Linux/Unix/BSD

- Jenis
- Versi
- Kernel

Cara:

Pada skrin terminal taip ***uname –a***

g) Apakah kegunaan server terbabit?

i. Web server

- Jenis

  Contoh:
  - *Microsoft IIS*
  - *Apache*
  - *Netscape*
  - *Lotus*
  - Lain-lain (Nyatakan)

ii. E-mel server

- Jenis

  Contoh:
  - *Microsoft Exchange*
  - *Sendmail (Unix)*
  - *Qmail (Unix)*
  - *Postfix (Unix)*
  - *Lotus*
  - Lain-lain (Nyatakan)

iii. Sistem aplikasi/perkhidmatan lain

- Jenis

  Contoh:
  - Aplikasi dalaman
  - Aplikasi web
  - Pangkalan data
  - *Web Portal*
  - DNS

iv. Lain-lain (Nyatakan)

- Jenis

h) Maklumat *hard disk* (jika berkenaan)

i. Kapasiti

ii. Jenis *hard disk*

Cara untuk mendapatkan kapasiti *hard disk* adalah seperti berikut:

a) Win NT/Win 2000/Win 2003

- ***Klik Start > Program > Administrative Tools > Disk Administrator***

b) Linux/Unix/BSD

- ***Pada skrin terminal , taip df-h (generic command)***
- ***Taip flag –h (Unix)***

i) Adakah server terbabit berhubung dengan lain- lain perkakasan atau server di rangkaian (*internet/intranet*) atau *standalone*?

Jika YA, dapatkan maklumat server tersebut.

j) Adakah rangkaian tersebut dilengkapi dengan benteng pertahanan seperti Firewall/*IDS/IPS*? Jika YA, dapatkan maklumat tersebut:

i. *Firewall*

- Jenis
- Versi
- Diselenggara oleh pembekal/sendiri

ii. *Intrusion Detection System/Intrusion Protection System* (IDS/IPS)

- Jenis
- Versi
- Diselenggara oleh pembekal/sendiri

	iii. *Router* • Jenis • Versi • Diselenggara oleh pembekal/sendiri k) Adakah server tersebut dilengkapi oleh perisian antivirus? Jika YA, dapatkan maklumat antivirus tersebut • Jenis • Kekerapan mengemaskini (*update*) *signature* • Tarikh *virus signature* terkini
4.0	**Tindakan Yang Diambil Oleh Agensi** a) Boleh tuan/puan terangkan tindakan-tindakan yang telah dijalankan? b) Adakah server tersebut masih dihubungkan pada rangkaian? (Jika berkenaan) c) Adakah pihak tuan/puan mempunyai salinan imej (*backup*) data ke atas *server* yang diceroboh? i. Apakah bentuk media salinan (*backup*) *Contoh:* • *Hard disk* berasingan (*Separate hard disk*) • *Cartridge* • *Optical Disk* • Imej *backup* • Lain-lain **Nota:** Tujuan *backup* adalah untuk proses *restore* data selepas dibaikpulih d) Adakah terdapat **maklumat terperingkat** di dalam server tersebut? e) Adakah server di agensi tuan/puan pernah diceroboh/diserang sebelum ini? Jika YA, dapatkan maklumat lanjut. f) Adakah server tersebut telah dijalankan langkah-langkah pengukuhan (*patches*) sebelum ini? Jika YA, i. Dapatkan tarikh terakhir langkah-langkah pengukuhan dijalankan. ii. Apakah *patches* yang telah dilaksanakan? g) Apakah lain-lain tindakan yang telah diambil oleh agensi tuan/puan? *Contoh:* i. Melapor kepada GCERT/MyCERT ii. Melapor kepada Pembekal iii. Melapor kepada Pihak Penguatkuasa (PDRM)

5.0 **Nasihat Awal**

a) Adakah tuan/puan telah memutuskan hubungan sistem/server?

(Bergantung kepada jenis insiden, nasihat awal adalah bertujuan untuk mengawal insiden daripada merebak)

Contoh:

i. Sekiranya insiden *unauthorized access*, putuskan sambungan UTP port dari server terbabit

ii. Sekiranya *virus* atau *worm*, ikut nasihat dari pembekal/CERT Advisories

iii. Sekiranya *E-mail Spamming*, semak konfigurasi *e-mail relay* dan *Disable email relay* untuk hentikan perkhidmatan

b) i. Jika berkenaan, dapatkan fail –fail log.

Boleh tuan/puan kemukakan fail-fail log 5 hari (sebelum dan semasa tarikh insiden) melalui email CERT Agensi (cert@agensi.gov.my) / (cert_subagensi@agensi.gov.my)

Cara mendapatkan fail log adalah seperti berikut:

i. Win NT/Win 2000/Win 2003

- **Web Access Log**

  C:\WINNT\System32/Log Files\W3SVC2

  Atau

  C:\WINNT\System32/Log Files\W3SVC3

- **Event Log Win NT/Win 2000 (default)**

  C:\Winnt\System32\Event log

  - **system.evt**
  - **application.evt**
  - **security.evt**
  - ***.evt**

ii. Untuk membolehkan penghantaran ke CERT Agensi secara elektronik (cert@agensi.gov.my) / (cert_subagensi@agensi.gov.my), agensi perlu ‘compress’/zip fail-fail log tersebut.

Cara untuk *compress/zip* fail:

i. Win NT/ Windows 2000/Win 2003

- **Menggunakan aplikasi winzip**

ii. Unix/Linux/BSD

- **tar –cvf log.tar /var/log/ atau**
- **tar –cvf log.tar /var/adm/log**

  gzip log.tar

Fail baru yang dihasilkan ialah log.tar

iii. Untuk makluman tuan/puan, selepas fail-fail log diterima, CERT Agensi akan jalankan analisa fail-fail log tersebut dan hasilnya akan dimajukan kepada pihak tuan/puan dengan kadar SEGERA (jika berkenaan)

c) Sekiranya berkenaan, tuan/puan disarankan untuk menjalankan langkah-langkah pengukuhan (*patches*). Boleh merujuk pada:

- Laman web ICT Security (**http://www.ictsecurity.gov.my**)

d) Tuan/puan dinasihatkan supaya menjalankan salinan (*backup*) ke atas sistem yang diceroboh (sekiranya perlu)

e) Tuan/puan juga dinasihatkan menjalankan pemeriksaan berikut ke atas server lain yang berada di dalam rangkaian yang sama (sekiranya perlu)

Contoh:

- Semak kandungan fail log
- Semak *directory*
- Semak *temporary file*

f) i. Sebagai tindakan susulan, CERT Agensi memohon kerjasama tuan/puan untuk mengemukakan Borang Laporan Pengendalian Insiden iaitu Borang IRH 1.0

Nota:

Borang IRH 1.0 boleh diperolehi melalui laman web ICT Security pada URL **http://agensi.gov.my**

ii. Borang yang telah lengkap diisi bolehlah dikemukakan kepada CERT Agensi samada melalui e-mel CERT Agensi (**cert@agensi.gov.my**) / (**cert_subagensi@agensi.gov.my**) atau melalui faks.

	g) (Jika berkenaan) Selepas fail-fail log diterima, CERT Agensi akan jalankan analisa fail-fail log tersebut dan hasilnya akan dimajukan kepada pihak tuan/puan SECEPAT MUNGKIN. h) Bolehkah tuan/puan maklumkan dengan SEGERA kepada CERT Agensi sekiranya semua langkah-langkah pengukuhan telah selesai supaya dapat dijalankan *Host Scanning*. Tujuannya adalah untuk menentukan tahap keselamatan server terbabit.
6.0	**PENUTUP** a) Ucapkan terima kasih b) Minta kerjasama daripada agensi supaya mengikuti nasihat yang telah diberikan. c) Sekiranya mempunyai sebarang masalah/ memerlukan bantuan, minta agensi hubungi CERT Agensidi nombor dan email seperti berikut: i. Nombor Telefon: _____ (Pengurus CERT Agensi) ii. Nombor telefon Pegawai CERT Agensi yang mengendalikan insiden : iii. E-mel CERT Agensi : **(**cert@agensi.gov.my**) /** **(**cert_subagensi@agensi.gov.my**)**

<NAMA AGENSI> **File : <Nama fail log.log>**

Template Laporan Analisa Log

Case ID : <NO. INSIDEN>/TAHUN

Bil.	Alamat IP Penyerang	Masa	Aktiviti
1.	Senaraikan alamat IP penyerang	Catatkan masa yang terlibat	Senaraikan jenis *vulnerability* yang ada dan *script* yang terlibat (dalam fail log)
2.			

Rujukan Fail CERT Agensi-Tarikh

SINGKATAN PERKATAAN

CIA	-	*Confidentiality*, *Integrity and Availaility*
CIO	-	*Chief Information Officer*
GCERT	-	*Government Computer Emergency Response Team*
CERT Agensi	-	*Computer Emergency Response Team* di Agensi
ICT	-	*Information and Communication Technology*
ICTSO	-	*ICT Security Officer*
ID	-	*Identification*
IDS	-	*Intrusion Detection System*
IP	-	*Internet Protocol*
IPS	-	*Intrusion Protection System*
IRH	-	*Incident Response Handling*
LAN	-	*Local Area Network*
MyCERT	-	*Malaysian Computer Emergency Response Team*
SANS	-	*Sans Consulting Services Inc.*
SOP	-	*Standard Operating Procedure*
URL	-	*Universal Resource Locater*