



**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 menyediakan 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 mengendalikan 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](mailto:gcert@mampu.gov.my)
- (c) Telefon : 012-3312205
- (d) Nombor Faksimili : 03-88883286

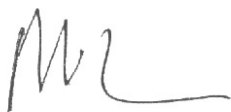
## PEMAKAIAN

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

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

**GARIS PANDUAN  
PENGURUSAN PENGENDALIAN INSIDEN  
KESELAMATAN ICT  
SEKTOR AWAM**

## KANDUNGAN

## MUKA SURAT

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

# 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) **Penceroobohan (*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**

Percubaan (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, menjejaskan 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 mengendalikan 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

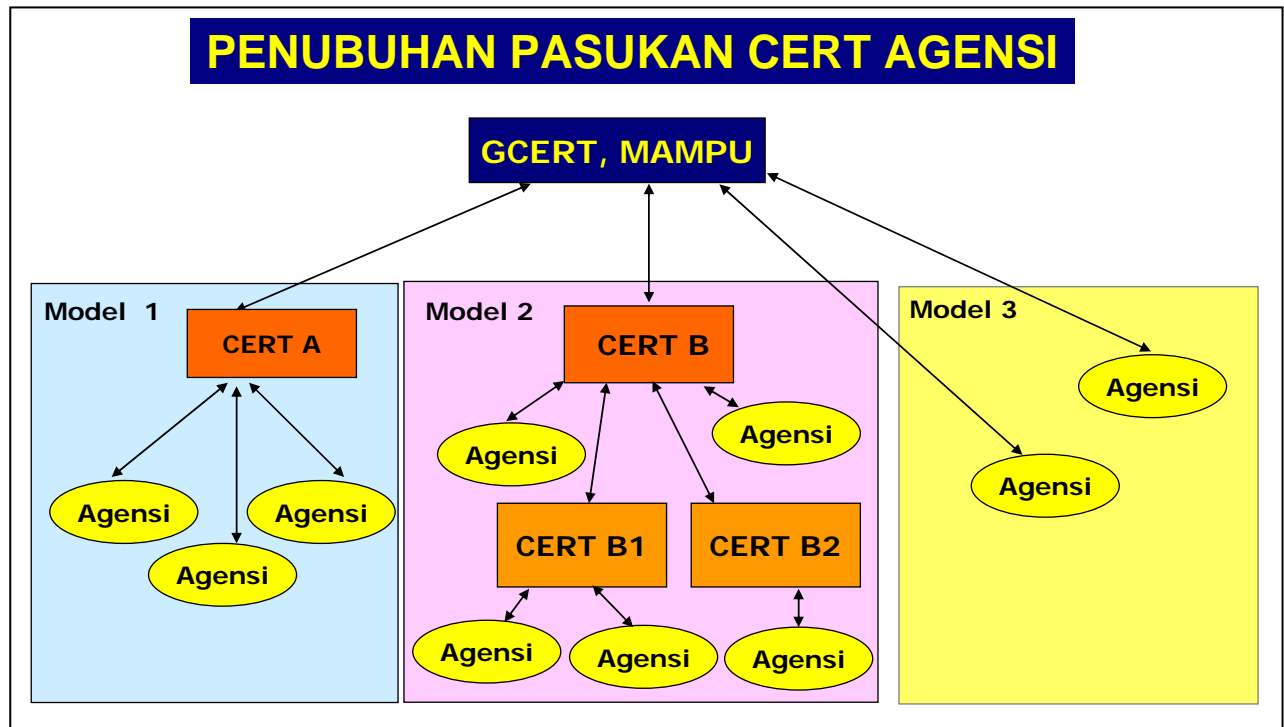
Menerusi model 2, beberapa pasukan pengurus insiden ditubuhkan di peringkat jabatan atau agensi. Pasukan-pasukan ini kemudian diselaraskan di peringkat pusat CERT yang ditubuhkan di peringkat kementerian.

c) Model 3

Model ini terpakai kepada agensi-agensi yang kecil yang tidak mempunyai anggota teknikal yang mencukupi untuk mengendalikan 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 menyebarkan maklumat mengenai ancaman baru dari masa ke semasa;
- (c) Menyediakan khidmat nasihat kepada CERT Agensi berkaitan dengan pengurusan dan pengendalian 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.

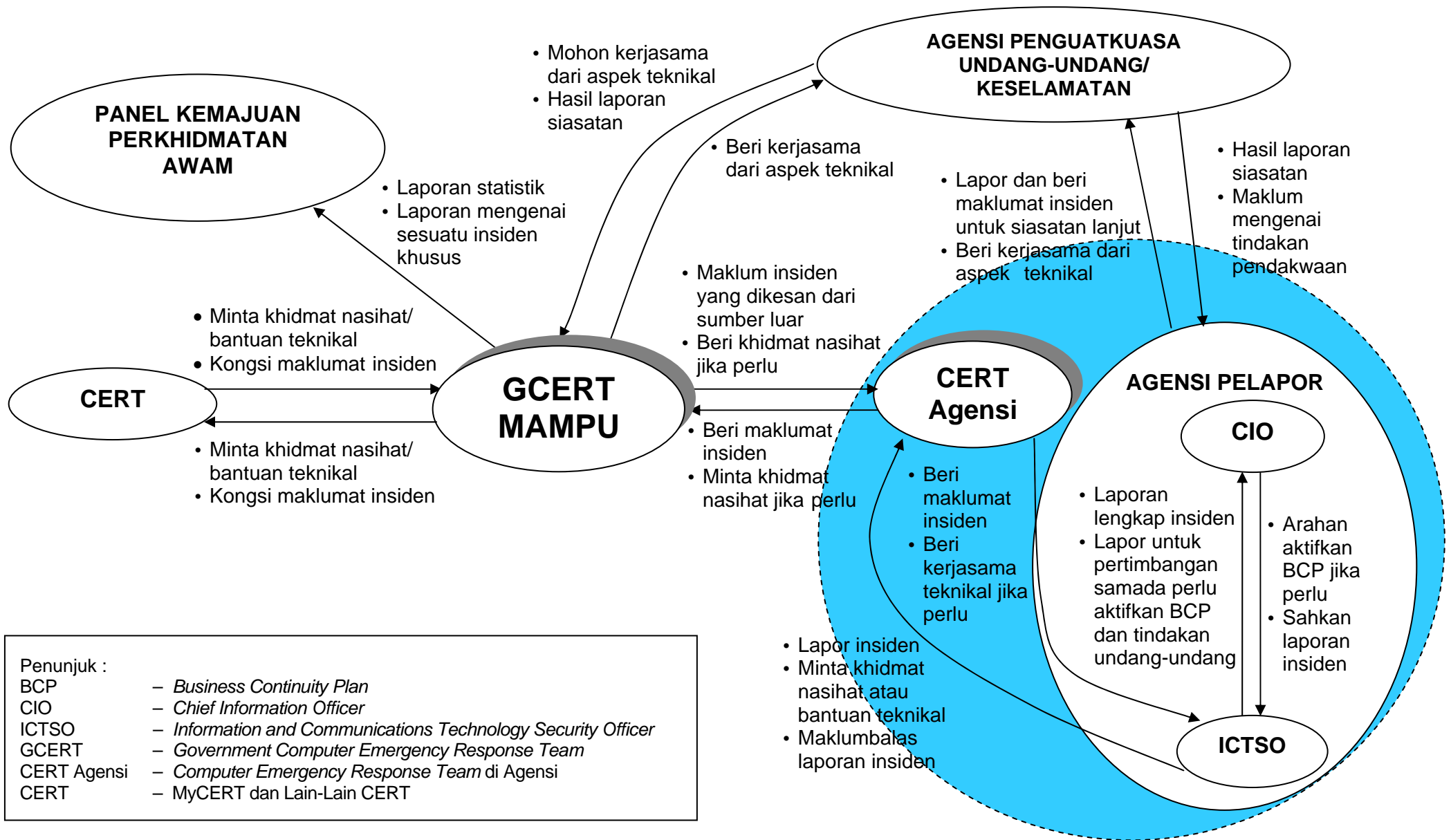
15. GCERT MAMPU juga bertanggungjawab kepada agensi-agensi kecil (struktur CERT Model 3) dalam mengurus pengendalian insiden keselamatan ICT seperti berikut :

- (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**

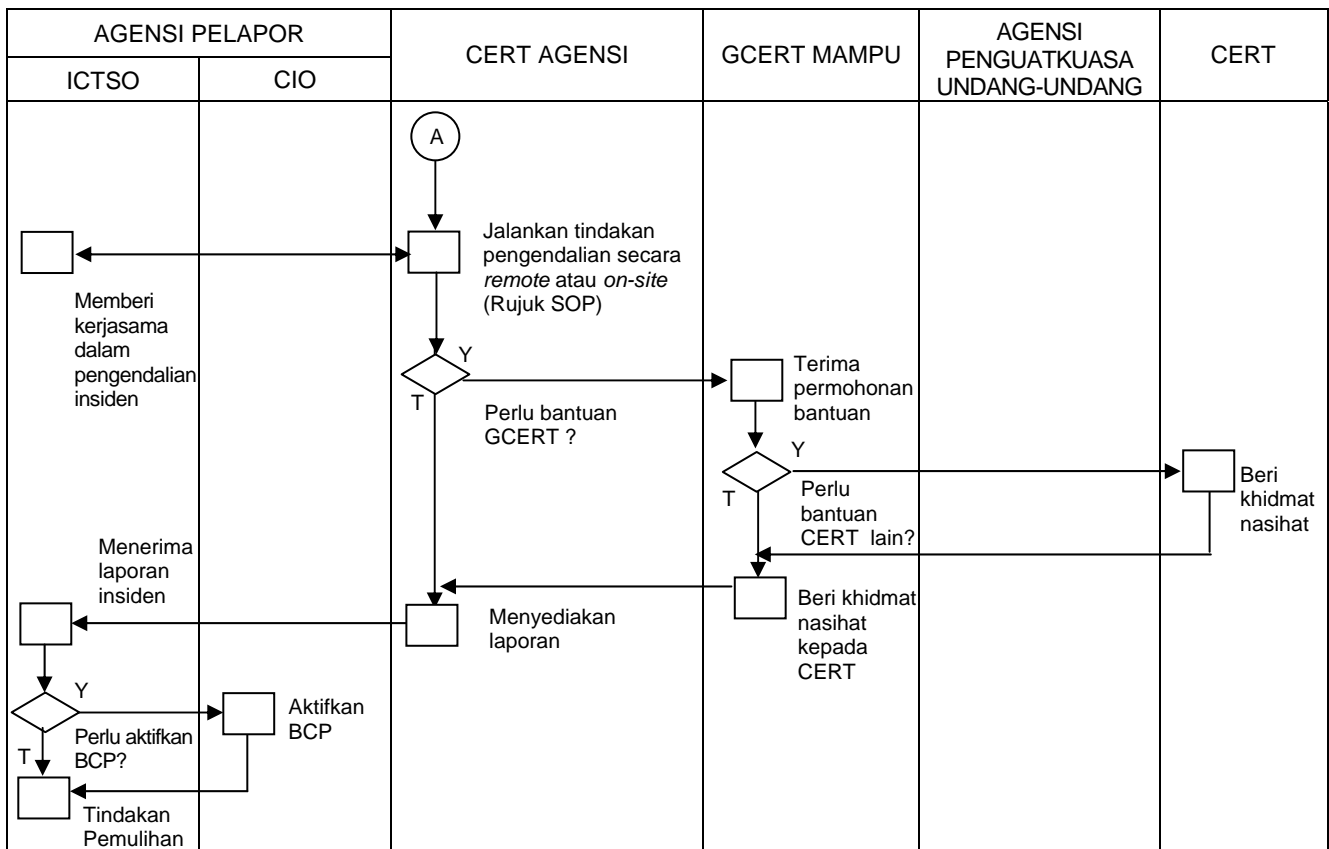
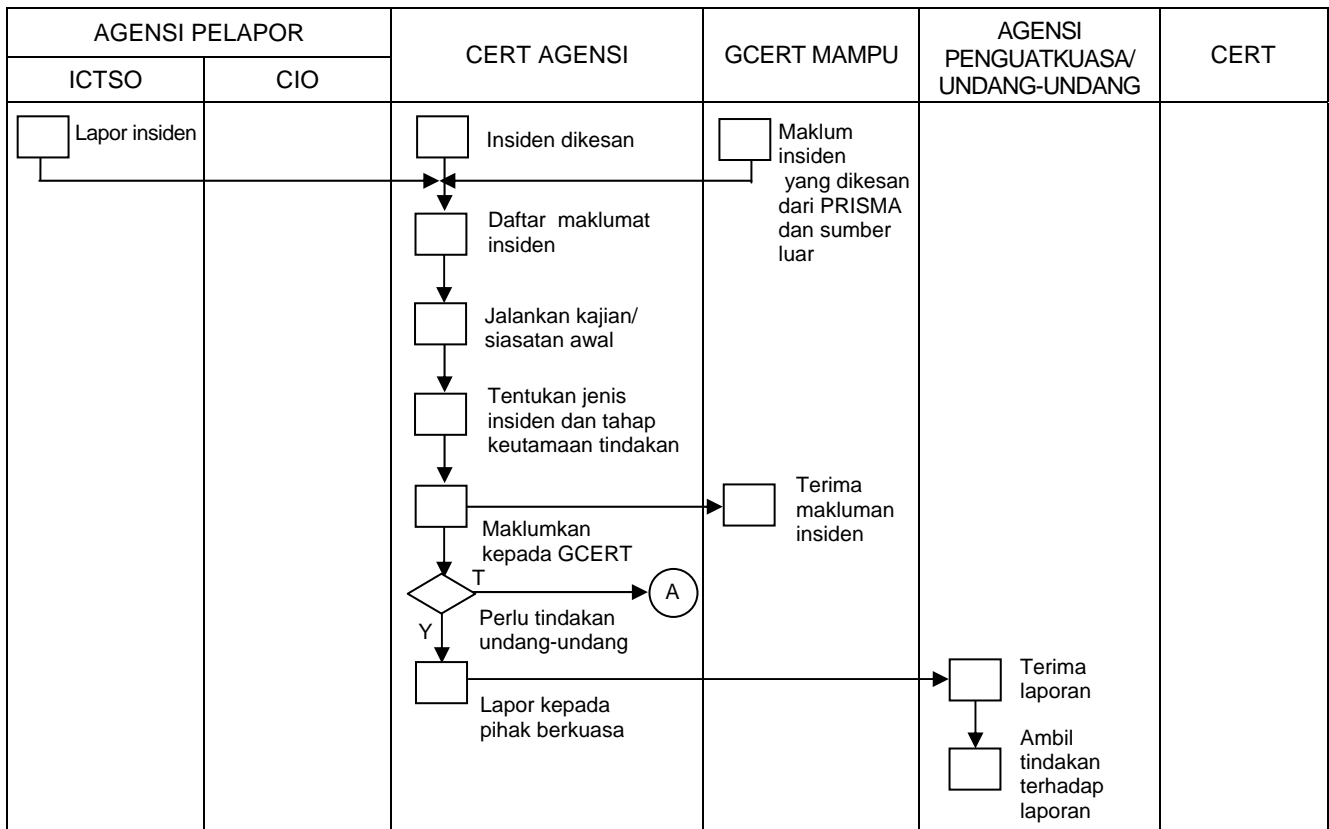
16. Proses Pelaporan Insiden Keselamatan ICT Sektor Awam diringkaskan dalam **Rajah 2 – Hubungan Entiti Dalam Proses Kerja Pelaporan Insiden Keselamatan ICT** dan **Rajah 3 – Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT** di bawah. Proses pengendalian insiden keselamatan ICT diterangkan secara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

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

**PROSEDUR OPERASI STANDARD  
PENGURUSAN PENGENDALIAN INSIDEN  
KESELAMATAN ICT  
CERT AGENSI**

## KANDUNGAN

## MUKA SURAT

1.	OBJEKTIF	1
2.	PROSEDUR OPERASI STANDARD	1
	- Pentadbiran <i>Incident Response Handling</i> (IRH)	1
	- Pengurusan Pengendalian Insiden	2
	- Pengendalian Insiden Secara Jarak Jauh ( <i>Remote</i> )	4
	- Pengendalian Insiden Di Lokasi Agensi Terlibat ( <i>On site</i> )	7
	- Penyebaran Maklumat	13
	- Penyelarasan Pengurusan Insiden Keselamatan ICT	14
3.	LAMPIRAN	
	- Panduan Komunikasi Pengendalian Insiden Secara Jarak Jauh	15
	- Template Borang IRH 1.0 : Maklumat Pengendalian Insiden Keselamatan ICT	22
	- Template Borang IRH 1.1 : Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT	24
	- Template Laporan Analisis Fail Log	26
	- Template Laporan Imbasan Hos	27
	- Template Laporan Kronologi Insiden Keselamatan ICT	28
	- Singkatan Perkataan	29

# PROSEDUR OPERASI STANDARD PENGURUSAN 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 masa 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 - Catat maklumat awal insiden**

Keterangan Aktiviti	Mekanisme/Rujukan	Tindakan
1. Setiap aduan yang diterima perlu dicatatkan dalam borang, buku log/ fail atau pangkalan data berkaitan.	<ul style="list-style-type: none"><li>Buku/ fail/ sistem Log</li><li>Borang IRH 1.0 – Maklumat Pengendalian Insiden Keselamatan ICT</li></ul>	<ul style="list-style-type: none"><li>Pegawai CERT Agensi</li></ul>

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

**Tugas 2.1 - Tadbir dan selenggara fail-fail insiden**

Keterangan Aktiviti	Mekanisme/Rujukan	Tindakan
1. Sekiranya catatan dibuat ke dalam borang, failkan borang berkenaan dan kemaskini rekod statistik insiden.	<ul style="list-style-type: none"><li>Borang IRH 1.0 – Maklumat Pengendalian Insiden Keselamatan ICT</li><li>Statistik insiden</li><li>Surat</li><li>E-mail</li><li>Faks</li><li>Fail Sulit</li></ul>	<ul style="list-style-type: none"><li>Pegawai CERT Agensi</li></ul>
2. Simpan maklumat/dokumen yang berkaitan ke dalam server dengan mengambil kira perkara-perkara berikut : a) <i>Encrypt</i> maklumat /dokumen insiden; dan b) Dokumen disimpan mengikut nama direktori agensi masing-masing (CERT Fail Server/ nama_agensi/no_insiden-nama_pegawai).	<ul style="list-style-type: none"><li>Fail Server CERT Agensi</li></ul>	<ul style="list-style-type: none"><li>Pegawai CERT Agensi</li></ul>

**Proses 3 - Kemaskini Maklumat Insiden Selepas Siasatan**

**Tugas 3.1 - Kemaskini maklumat insiden selepas siasatan**

Keterangan Aktiviti	Mekanisme/Rujukan	Tindakan
1. Kemaskini maklumat insiden yang diperolehi semasa siasatan ke dalam fail-fail/pangkalan data insiden.	<ul style="list-style-type: none"><li>Fail Server/Media CERT Agensi</li></ul>	<ul style="list-style-type: none"><li>Pegawai CERT Agensi</li></ul>

**4. Pengurusan Pengendalian Insiden**

- Jalankan kajian atau siasatan awal insiden
- Tentukan jenis dan tahap keutamaan tindakan insiden
- Agihkan tugas dan kaedah pengendalian insiden



**Proses 4 - Jalankan Kajian Atau Siasatan Awal Insiden****Tugas 4.1 - Jalankan 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.	<ul style="list-style-type: none"> <li>Panduan Komunikasi Pengendalian Insiden Secara Jarak Jauh</li> </ul>	<ul style="list-style-type: none"> <li>2 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Semak laman web yang menyenaraikan insiden pencerobohan ke atas laman web kerajaan Malaysia.	<ul style="list-style-type: none"> <li>Rujuk laman web: <a href="http://www.zone-h.org">http://www.zone-h.org</a></li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> <li>Pegawai CERT Agensi</li> </ul>

**Proses 5 - Tentukan Jenis Dan Tahap Keutamaan Tindakan Insiden****Tugas 5.1 - Tentukan 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.	<ul style="list-style-type: none"> <li>Panduan Komunikasi Pengendalian Insiden Secara Jarak Jauh</li> <li>Borang IRH 1.0 – Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Berikan nasihat awal dan langkah-langkah untuk mendapatkan fail log terlibat.	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
3. Maklum dan berbincang dengan Pengurus CERT Agensi untuk agihan tugas pengendalian dan penentuan tahap keutamaan tindakan.	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> <li>Pegawai CERT Agensi</li> </ul>
4. Maklumkan insiden kepada GCERT MAMPU.	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> <li>Pegawai CERT Agensi</li> </ul>

**Proses 6 - Agihkan Tugas Dan Kaedah Pengendalian Insiden****Tugas 6.1 - Agihkan tugas pengendalian insiden**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Semak status pengendalian insiden semasa.	<ul style="list-style-type: none"> <li>Fail atau pangkalan data pengurusan pengendalian insiden</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
2. Agihkan tugas dan kaedah pengendalian insiden kepada pegawai CERT Agensi.	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> <li>Pegawai CERT Agensi</li> </ul>

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

- (a) Jalankan siasatan lanjut secara jarak jauh (*remote*)
- (b) Penyediaan laporan analisis fail-fail log
- (c) Pelaksanaan imbasan hos
- (d) Tindakan pemulihan
- (e) Penutupan kes insiden
- (f) Kemaskini maklumat dan status insiden

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

**Tugas 7.1 - Jalankan siasatan lanjut dan pantau penghantaran fail log agensi**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Jalankan siasatan lanjut mengenai insiden berkenaan.	<ul style="list-style-type: none"> <li>Borang IRH 1.0 – Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>2 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Pantau dan hubungi pegawai di agensi untuk penghantaran fail-fail log agensi.	<ul style="list-style-type: none"> <li>Borang IRH 1.0 – Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

**Proses 8 - Penyediaan Laporan Analisis Fail-Fail Log**

**Tugas 8.1 - Sediakan laporan analisis fail-fail log dan kemukakan kepada agensi**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Analisis fail-fail log yang diterima.	-	<ul style="list-style-type: none"> <li>30 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Sediakan laporan analisis fail log dan cadangan tindakan pengukuhan untuk semakan dan pengesahan Pengurus CERT Agensi. (Dapatkan bantuan GCERT sekiranya perlu).	<ul style="list-style-type: none"> <li>Fail-fail log diperolehi dari agensi</li> <li>Laporan Analisis Fail Log</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

**Tugas 8.2 - Semak dan sahkan laporan analisis fail log**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Semak dan sahkan laporan analisis fail log dan cadangan tindakan pengukuhan.	<ul style="list-style-type: none"> <li>• Fail-Fail Log Diperolehi Dari Agensi</li> <li>• Laporan Analisis Fail Log</li> </ul>	<ul style="list-style-type: none"> <li>• Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>• Pengurus CERT Agensi</li> </ul>

**Tugas 8.3 - Kemukakan laporan analisis fail log kepada agensi**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Kemukakan laporan analisis fail log dan cadangan tindakan pengukuhan kepada agensi serta maklumkan mengenai pelaksanaan imbasan hos selepas lima (5) dari tarikh penerimaan laporan.	<ul style="list-style-type: none"> <li>• Laporan Analisis Fail Log</li> <li>• Cadangan Tindakan Pengukuhan</li> <li>• Makluman Mengenai Pelaksanaan Imbasan Hos</li> </ul>	<ul style="list-style-type: none"> <li>• Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>• Pegawai CERT Agensi</li> </ul>

**Proses 9 - Pelaksanaan Imbasan Hos**

**Tugas 9.1 - Jalankan imbasan hos dan sediakan laporan imbasan hos**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Laksanakan imbasan hos ke atas server agensi terlibat.	-	<ul style="list-style-type: none"> <li>• 2 hari</li> </ul>	<ul style="list-style-type: none"> <li>• Pegawai CERT Agensi</li> </ul>
2. Sediakan laporan imbasan hos untuk semakan dan pengesahan Pengurus CERT Agensi.	<ul style="list-style-type: none"> <li>• Laporan Imbasan Hos</li> </ul>	<ul style="list-style-type: none"> <li>• 3 hari</li> </ul>	<ul style="list-style-type: none"> <li>• Pegawai CERT Agensi</li> </ul>

**Tugas 9.2 - Semak dan sahkan laporan imbasan hos**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Semak dan sahkan atau beri maklumbalas mengenai laporan imbasan hos.	<ul style="list-style-type: none"> <li>• Laporan Imbasan Hos</li> </ul>	<ul style="list-style-type: none"> <li>• Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>• Pengurus CERT Agensi</li> </ul>

**Tugas 9.3 - Kemukakan laporan imbasan hos kepada agensi**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Kemukakan laporan imbasan hos kepada agensi dan minta agensi kembalikan Borang IRH 1.1 yang telah dikemaskini selepas 5 hari laporan diterima oleh agensi.	<ul style="list-style-type: none"> <li>• Laporan Imbasan Hos</li> <li>• Borang IRH 1.1 - Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>• Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>• Pegawai CERT Agensi</li> </ul>

**Proses 10 - Tindakan Pemulihan****Tugas 10.1 - Tindakan pemulihan oleh agensi pelapor**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Laksanakan tindakan pemulihan berdasarkan laporan imbasan hos.	<ul style="list-style-type: none"> <li>Laporan Imbasan Hos</li> </ul>	<ul style="list-style-type: none"> <li>5 hari</li> </ul>	<ul style="list-style-type: none"> <li>Agensi Pelapor</li> </ul>

**Tugas 10.2 - Tindakan pemantauan pemulihan ke atas agensi pelapor**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Pantau pelaksanaan tindakan pemulihan oleh agensi pelapor berdasarkan laporan imbasan hos.	<ul style="list-style-type: none"> <li>Laporan Imbasan Hos</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

**Proses 11 - Penutupan Kes Insiden****Tugas 11.1 - Penutupan kes insiden**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Pantau penerimaan Borang IRH 1.1	<ul style="list-style-type: none"> <li>Borang IRH 1.1 - Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>2 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Mohon penutupan kes insiden sekiranya maklumbalas diterima dari Borang IRH 1.1 agensi menyatakan bahawa tindakan pengukuhan telah dilaksanakan.	<ul style="list-style-type: none"> <li>Borang IRH 1.1 - Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
3. Beri kelulusan menutup kes, sekiranya Pengurus CERT Agensi berpuashati dengan maklumbalas diterima.	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>
4. Maklumkan kepada GCERT mengenai penutupan kes.	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> <li>Pengurus CERT Agensi</li> </ul>

**Proses 12 - Kemaskini Maklumat Dan Status Insiden****Tugas 12.1 - Kemaskini 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.	<ul style="list-style-type: none"> <li>Fail/Pangkalan Data Insiden</li> <li>Statistik Insiden</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

## 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) Kemukakan laporan akhir insiden kepada agensi pelapor
- (g) Penutupan kes

### Proses 13 - Jalankan Siasatan Lanjut Di Lokasi (On-Site)

#### Tugas 13.1 - Hubungi agensi untuk dapatkan maklumat lanjut dan membuat temu janji dengan agensi

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Hubungi agensi terlibat untuk mendapatkan : a) maklumat lanjut b) memberi nasihat awal		<ul style="list-style-type: none"> <li>2 hari</li> <li>(* Tempoh pengendalian bergantung sama ada agensi berjaya/gagal dihubungi)</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Dapatkan 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.	<ul style="list-style-type: none"> <li>Borang IRH 1.0 - Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
3. Maklumkan kepada Pengarah CERT Agensi secara lisan atau e-mel bahawa CERT Agensi akan menjalankan siasatan lanjut di lokasi ( <i>on-site</i> ).	<ul style="list-style-type: none"> <li>Borang IRH 1.0 - Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>
4. Dapatkan kebenaran untuk keluar stesen jika perlu.	<ul style="list-style-type: none"> <li>Borang Keluar Stesen</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

#### Tugas 13.2 - Sediakan kelengkapan pengendalian insiden

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Sediakan kelengkapan seperti berikut : a) <i>Notebook</i> ; b) Borang yang berkaitan; c) <i>Disket/Thumb Drive</i> ; d) <i>Hard disk</i> ; dan e) Perisian dan peralatan forensik.	<ul style="list-style-type: none"> <li>Borang IRH 1.0 - Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
2. Pastikan semua kelengkapan pengendalian insiden adalah mencukupi.	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>

## Proses 14 - Mesyuarat Pengurusan IRH Di Agensi

### Tugas 14.1 - Jalankan mesyuarat pengurusan IRH dengan agensi

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
<p>1. Mesyuarat IRH dihadiri oleh :</p> <p>a) Agensi pelapor</p> <p>i. Ketua Jabatan/Ketua Bahagian IT</p> <p>ii. ICTSO</p> <p>iii. Pentadbir Sistem</p> <p>b) CERT Agensi</p> <p>i. Pengarah CERT Agensi</p> <p>ii. Pengurus CERT Agensi</p> <p>iii. Pegawai CERT Agensi</p> <p>c) Wakil GCERT (sekiranya perlu)</p>	<ul style="list-style-type: none"> <li>Borang IRH 1.0 - Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>1 hari</li> </ul>	<ul style="list-style-type: none"> <li>Agensi pelapor</li> <li>Pengarah CERT Agensi (sekiranya perlu)</li> <li>Pengurus CERT Agensi</li> <li>Pegawai CERT Agensi</li> </ul>
<p>2. Perbincangan mesyuarat meliputi :</p> <p>a) Tujuan IRH di lokasi (<i>On-site</i>).</p> <p>b) Dapatkan maklumat lanjut pencerobohan</p> <p>c) Maklumkan proses-proses IRH</p> <p>d) Laporkan kepada Pihak Penguatkuasa PDRM (sekiranya perlu) dan CERT Agensi akan membantu penyiasatan sekiranya diperlukan.</p>	<ul style="list-style-type: none"> <li>Borang IRH 1.0 - Maklumat Pengendalian Insiden Keselamatan ICT</li> <li>Laporan Kronologi Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>1 hari</li> </ul>	<ul style="list-style-type: none"> <li>Agensi pelapor</li> <li>Pengarah CERT Agensi (sekiranya perlu)</li> <li>Pengurus CERT Agensi</li> <li>Pegawai CERT Agensi</li> </ul>
<p>3. Catatkan keseluruhan proses kronologi insiden keselamatan ICT bermula dari mesyuarat dijalankan sehingga proses pengendalian insiden tersebut selesai.</p>	<ul style="list-style-type: none"> <li>Laporan Kronologi Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

**Proses 15 - Siasatan Terperinci *Incident Response Handling* (IRH)**

**Tugas 15.1 - Jalankan siasatan terperinci**

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
<p>1. Jalankan siasatan lanjut ke atas sistem/<i>server</i> yang diceroboh (bergantung kepada keperluan) seperti berikut :</p> <p>a) Dapatkan data forensik;</p> <p>b) Buat 2 salinan ke <i>atas hard disk</i>;</p> <p>c) Asingkan perkakasan yang diceroboh (<i>quarantine</i>)</p> <p>d) Salin fail-fail log sistem, aplikasi dan firewall;</p> <p>e) Cari fail-fail hasil tinggalan penceroboh seperti <i>backdoor, trapdoor, trojan horse, virus</i> dan <i>worm</i>;</p> <p>f) Jalankan <i>port scanning</i>;</p> <p>g) Jalankan <i>vulnerability scanning</i>; dan</p> <p>h) <i>File Usage Activity</i>.</p>	<ul style="list-style-type: none"> <li>Perisian Dan Peralatan Forensik</li> <li>Laporan Kronologi Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>7 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> <li>Pengurus CERT Agensi</li> </ul>
<p>2. Analisis maklumat/bukti-bukti pencerobohan yang diperolehi hasil daripada siasatan lanjut ke atas sistem/<i>server</i> yang diceroboh.</p>	<ul style="list-style-type: none"> <li>Sumber Internet</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> <li>Pegawai CERT Agensi</li> </ul>
<p>3. Maklumkan kepada agensi pelapor secara lisan mengenai tindakan dan status siasatan sistem/<i>server</i> yang diceroboh dari masa ke semasa.</p>	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> <li>Pegawai CERT Agensi</li> </ul>

**Tugas 15.2 - Jalankan proses baik pulih**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
<p>1. Jalankan aktiviti-aktiviti seperti berikut :</p> <p>a) Format semula sistem/<i>server</i> yang diceroboh (jika perlu);</p> <p>b) <i>Install</i> semula sistem pengoperasian;</p> <p>c) <i>Install</i> perisian anti-virus dengan <i>signature</i> terkini; dan</p> <p>d) <i>Restore</i> menggunakan <i>backup</i> data</p>	-	<ul style="list-style-type: none"> <li>7 hari</li> </ul>	<ul style="list-style-type: none"> <li>Agensi pelapor</li> </ul>

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
<p>2. Sekiranya sistem/server tidak perlu diformat :</p> <p>a) Jalankan <i>backup</i> ke atas sistem;</p> <p>b) Tukar kata laluan yang sedia ada kepada yang lebih selamat Contohnya: Gabungkan simbol + huruf + nombor);</p> <p>c) Hapuskan fail-fail hasil tinggalan penceroboh seperti <i>backdoor</i>, <i>trapdoor</i>, <i>trojan horse</i>, <i>virus</i> atau <i>worm</i>;</p> <p>d) <i>Restore</i> menggunakan <i>backup</i> data; dan</p> <p>e) <i>Install</i> atau kemas kini perisian anti-virus dengan <i>signature</i> terkini.</p>	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Agensi pelapor</li> </ul>
<p>3. Beri khidmat nasihat kepada agensi pelapor mengenai langkah-langkah pengukuhan dan tindakan yang perlu diambil dari masa ke semasa.</p>	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> <li>Pegawai CERT Agensi</li> </ul>

### Proses 16 - Penyediaan Laporan Awal Pentadbiran CERT Agensi

#### Tugas 16.1 - Sediakan laporan awal pentadbiran CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
<p>1. Sediakan laporan awal hasil siasatan IRH di lokasi (<i>On-site</i>) untuk makluman pihak pengurusan atasan agensi di CERT Agensi (Ketua Jabatan).</p>	<ul style="list-style-type: none"> <li>Laporan Awal Siasatan CERT Agensi</li> <li>Borang IRH 1.0 – Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>3 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

#### Tugas 16.2 - Pengesahan dan kelulusan laporan awal pentadbiran CERT Agensi

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
<p>1. Semak dan sahkan laporan awal siasatan CERT Agensi.</p>	<p>Laporan Awal Siasatan CERT Agensi</p>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>
<p>2. Pertimbang dan luluskan laporan awal siasatan CERT Agensi yang lengkap.</p>	<ul style="list-style-type: none"> <li>Laporan Awal Siasatan CERT Agensi</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengarah CERT Agensi</li> </ul>



**Tugas 16.3 - Kemukakan laporan awal pentadbiran CERT Agen kepada pihak pengurusan CERT Agensi**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Kemuka dan terangkan secara ringkas laporan awal siasatan CERT Agensi kepada pihak pengurusan atasan agensi di CERT Agensi (Ketua Jabatan)	<ul style="list-style-type: none"> <li>Laporan Awal Siasatan CERT Agensi</li> </ul>	<ul style="list-style-type: none"> <li>1 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pengarah CERT Agensi</li> <li>Pengurus CERT Agensi</li> </ul>

**Proses 17 - Penyediaan Laporan Insiden**

**Tugas 17.1 - Sediakan laporan dan slaid pembentangan insiden pencerobohan**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Kemaskini dan sediakan laporan kronologi insiden keselamatan ICT yang sedia ada, laporan teknikal yang terperinci dan slaid pembentangan insiden pencerobohan untuk semakan dan pengesahan Pengurus CERT Agensi.	<ul style="list-style-type: none"> <li>Laporan Kronologi Insiden Keselamatan ICT</li> <li>Laporan Insiden Pencerobohan Keselamatan ICT (Teknikal)</li> <li>Slaid Pembentangan Insiden Pencerobohan</li> </ul>	<ul style="list-style-type: none"> <li>14 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Sediakan laporan pengurusan untuk pihak Pengurusan Atasan agensi di CERT Agensi dan agensi dibawah tanggungjawab CERT Agensi.	<ul style="list-style-type: none"> <li>Laporan Insiden Pencerobohan Keselamatan ICT (Pengurusan)</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>

**Tugas 17.2 - Pengesahan dan kelulusan laporan insiden pencerobohan keselamatan ICT dan slaid pembentangan insiden pencerobohan**

Keterangan	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Semak dan sahkan laporan kronologi insiden keselamatan ICT, laporan insiden pencerobohan keselamatan ICT (Teknikal) dan slaid pembentangan insiden pencerobohan.	<ul style="list-style-type: none"> <li>Laporan Kronologi Insiden Keselamatan ICT</li> <li>Laporan Insiden Pencerobohan Keselamatan ICT (Teknikal)</li> <li>Slaid Pembentangan Insiden Pencerobohan</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>
2. Pertimbang dan luluskan laporan dan slaid pembentangan insiden pencerobohan keselamatan ICT (Pengurusan dan Teknikal).	<ul style="list-style-type: none"> <li>Laporan Insiden Pencerobohan Keselamatan ICT (Pengurusan dan Teknikal)</li> <li>Slaid Pembentangan Insiden Pencerobohan</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengarah CERT Agensi</li> </ul>

**Proses 18 - Kemukakan Laporan Akhir Insiden Kepada Agensi Pelapor****Tugas 18.1 - Hantar laporan akhir insiden pencerobohan keselamatan ICT (hardcopy) kepada agensi**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Sediakan surat untuk dilampirkan bersama laporan insiden pencerobohan keselamatan ICT kepada agensi pelapor untuk ditandatangani Pengurus CERT Agensi.	-	<ul style="list-style-type: none"> <li>1 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Kemukakan laporan akhir insiden pencerobohan keselamatan ICT (Pengurusan dan Teknikal) sebanyak tiga (3) salinan kepada: <ol style="list-style-type: none"> <li>Agensi pelapor;</li> <li>GCERT; dan</li> <li>Fail CERT Agensi.</li> </ol>	<ul style="list-style-type: none"> <li>Laporan Insiden Pencerobohan Keselamatan ICT (Pengurusan dan Teknikal)</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
3. Hantar dokumen laporan akhir insiden dengan mengikut prosedur surat SULIT.	<ul style="list-style-type: none"> <li>Buku Arahan Keselamatan</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
4. Hubungi agensi pelapor bagi memastikan dokumen Laporan IRH telah diterima.	-	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

**Proses 19 - Penutupan Kes****Tugas 19.1 - Bentang laporan akhir insiden pencerobohan keselamatan ICT kepada agensi**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Adakan temu janji bersama agensi pelapor bagi menjalankan pembentangan laporan insiden pencerobohan keselamatan ICT.	-	<ul style="list-style-type: none"> <li>1 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Bentangkan laporan insiden pencerobohan.	<ul style="list-style-type: none"> <li>Laporan Insiden Pencerobohan Keselamatan ICT (Pengurusan dan Teknikal)</li> <li>Slaid Pembentangan Insiden Pencerobohan</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>

**Tugas 19.2 - Kemaskini statistik insiden**

Keterangan	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Kemaskini statistik insiden pencerobohan untuk tujuan perekodan dan memasukkan dokumen yang berkaitan ke dalam fail SULIT.	<ul style="list-style-type: none"> <li>Statistik Insiden</li> <li>Fail Sulit</li> </ul>	<ul style="list-style-type: none"> <li>1 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>
2. Maklumkan kepada GCERT mengenai penutupan kes.		<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

## 7. Penyebaran Maklumat

- a) Dapatkan maklumat dari internet atau agensi lain
- b) Kajian terperinci terhadap ancaman dan impak insiden
- c) Sediakan nota makluman mengenai ancaman
- d) Sebar nota makluman kepada agensi

**Proses 20 - Dapatkan Maklumat Dari Internet Atau Agensi Lain**

**Tugas 20.1 - Dapat dan rekodkan maklumat dari internet atau aduan dari agensi**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Dapat dan rekod aduan dari agensi atau maklumat dari internet.	<ul style="list-style-type: none"> <li>• Buku/fail/sistem Log</li> <li>• Borang IRH 1.0 – Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>• 1 hari</li> </ul>	<ul style="list-style-type: none"> <li>• Pegawai CERT Agensi</li> <li>• Pengurus CERT Agensi</li> </ul>

**Proses 21 - Kajian Terperinci Terhadap Ancaman Dan Impak Insiden**

**Tugas 21.1 - Jalankan aktiviti kajian**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Jalankan analisis ke atas aduan atau maklumat yang diperolehi.	<ul style="list-style-type: none"> <li>• Sumber Internet</li> </ul>	<ul style="list-style-type: none"> <li>• 3 hari</li> </ul>	<ul style="list-style-type: none"> <li>• Pengawai CERT Agensi</li> </ul>
2. Dapatkan maklumat lanjut.	<ul style="list-style-type: none"> <li>• Agensi Terlibat</li> <li>• Sumber Internet</li> <li>• Sumber Lain</li> </ul>	<ul style="list-style-type: none"> <li>• Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>• Pengawai CERT Agensi</li> </ul>
3. Maklumkan kepada agensi mengenai status kajian dan tindakan yang perlu diambil.	<ul style="list-style-type: none"> <li>• Borang IRH 1.0 – Maklumat Pengendalian Insiden Keselamatan ICT</li> </ul>	<ul style="list-style-type: none"> <li>• Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>• Pengawai CERT Agensi</li> </ul>
4. Sediakan laporan terperinci mengenai insiden/ancaman keselamatan ICT, tahap kerosakan dan impak.	<ul style="list-style-type: none"> <li>• Laporan Terperinci Insiden/ Ancaman</li> </ul>	<ul style="list-style-type: none"> <li>• Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>• Pengawai CERT Agensi</li> </ul>

**Proses 22 - Sediakan Nota Makluman Mengenai Ancaman**

**Tugas 22.1 - Sediakan nota makluman mengenai ancaman**

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
1. Sediakan deraf nota makluman dan ringkasan mengenai insiden/ ancaman keselamatan ICT, tahap kerosakan dan impak.	<ul style="list-style-type: none"> <li>• Nota Makluman</li> <li>• Laporan Terperinci Insiden/ Ancaman</li> <li>• Laporan Ringkas</li> </ul>	<ul style="list-style-type: none"> <li>• 1 hari</li> </ul>	<ul style="list-style-type: none"> <li>• Pengawai CERT Agensi</li> </ul>

Keterangan Aktiviti	Mekanisme/ Rujukan	Tempoh Pengendalian	Tindakan
2. Buat semakan dan pengesahan nota makluman untuk dikemukakan kepada Pengarah CERT Agensi.	<ul style="list-style-type: none"> <li>Nota Makluman</li> <li>Laporan Ringkas</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>
3. Kemukakan nota makluman dan syor kaedah penyebaran makluman insiden/ancaman kepada Pengarah CERT Agensi.	<ul style="list-style-type: none"> <li>Nota Makluman</li> <li>Laporan Ringkas</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>
4. Buat keputusan mengenai tindakan penyebaran.	<ul style="list-style-type: none"> <li>Nota Makluman</li> <li>Laporan Ringkas</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengarah CERT Agensi</li> </ul>

### Proses 23 - Sebar Nota Makluman

#### Tugas 23.1 - Sebarkan nota makluman kepada ICTSO agensi di bawah kawalan

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Hantar e-mel kepada semua ICTSO agensi di bawah kawalan dan GCERT.	<ul style="list-style-type: none"> <li>Nota Makluman</li> <li>Laporan Ringkas</li> </ul>	<ul style="list-style-type: none"> <li>1 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pegawai CERT Agensi</li> </ul>

#### Tugas 23.2 - Kemukakan nota makluman kepada pihak pengurusan atasan agensi di CERT Agensi (jika perlu)

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Kemukakan nota makluman dan syor kaedah penyebaran makluman insiden/ancaman kepada pihak pengurusan atasan agensi di CERT Agensi.	<ul style="list-style-type: none"> <li>Nota Makluman</li> <li>Laporan Ringkas</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengarah CERT Agensi</li> </ul>
2. Keputusan mengenai tindakan penyebaran jika perlu.	<ul style="list-style-type: none"> <li>Nota Makluman</li> <li>Laporan Ringkas</li> </ul>	<ul style="list-style-type: none"> <li>Dalam tempoh yang sama seperti di atas</li> </ul>	<ul style="list-style-type: none"> <li>Pengurusan Atasan CERT Agensi</li> </ul>

## 8. Penyelarasan Pengurusan Insiden Keselamatan ICT

### Proses 24 - Penyelarasan Pengurusan Insiden Keselamatan ICT

#### Tugas 24.1 - Pengurusan mesyuarat penyelarasan insiden keselamatan ICT

Keterangan Aktiviti	Mekanisme / Rujukan	Tempoh Pengendalian	Tindakan
1. Adakan mesyuarat penyelarasan pengurusan keselamatan insiden ICT.	<ul style="list-style-type: none"> <li>Nota Cadangan</li> </ul>	<ul style="list-style-type: none"> <li>1 hari</li> </ul>	<ul style="list-style-type: none"> <li>Pengurus CERT Agensi</li> </ul>

A rectangular box with a black border containing the text "Logo CERT" in bold black font.

**Logo CERT**

**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	<p><b>Pengenalan</b></p> <p>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.</p> <p>b) Situasi 2: Agensi menghubungi CERT Agensi</p> <p><b>Nota:</b></p> <ul style="list-style-type: none"><li>• Kedua-dua situasi perlu merujuk kepada soalan-soalan di bawah :</li></ul>
2.0	<p><b>Maklumat Organisasi/Agensi</b></p> <p>a) Boleh saya dapatkan maklumat tuan/puan?</p> <ol style="list-style-type: none"><li>ICTSO<ul style="list-style-type: none"><li>• Nama</li><li>• Jawatan dan Gred</li><li>• No. Telefon Pejabat</li><li>• No. Telefon Bimbit</li><li>• E-mel</li></ul></li><li>Pentadbir Sistem<ul style="list-style-type: none"><li>• Nama</li><li>• Jawatan dan Gred</li><li>• No. Telefon Pejabat</li><li>• No. Telefon Bimbit</li><li>• E-mel</li></ul></li><li>Pegawai Untuk Dihubungi<ul style="list-style-type: none"><li>• Nama</li><li>• Jawatan dan Gred</li><li>• No. Telefon Pejabat</li><li>• No. Telefon Bimbit</li><li>• E-mel</li></ul></li></ol> <p><b>Nota:</b></p> <p>Telefon bimbit diperlukan supaya Pegawai bertanggungjawab mudah dihubungi di masa kecemasan atau di luar waktu pejabat</p> <p>b) Alamat Penuh Agensi</p> <ol style="list-style-type: none"><li>Boleh saya dapatkan alamat lengkap agensi tuan/puan?</li><li>Boleh saya tahu nama Bahagian yang bertanggungjawab?</li><li>Boleh saya tahu agensi tuan/puan di bawah Kementerian/Jabatan mana?</li></ol> <p>c) Nombor telefon agensi/Faks Boleh saya dapatkan nombor telefon agensi/faks di pejabat tuan/puan?</p>

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](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)

- Kapasiti
- 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.



	<p>j) Adakah rangkaian tersebut dilengkapi dengan benteng pertahanan seperti Firewall/IDS/IPS? Jika YA, dapatkan maklumat tersebut :</p> <p><b>i. Firewall</b></p> <ul style="list-style-type: none"> <li>• Jenis</li> <li>• Versi</li> <li>• Diselenggara oleh pembekal/sendiri</li> </ul> <p><b>ii. Intrusion Detection System/Intrusion Prevention System (IDS/IPS)</b></p> <ul style="list-style-type: none"> <li>• Jenis</li> <li>• Versi</li> <li>• Diselenggara oleh pembekal/sendiri</li> </ul> <p><b>iii. Router</b></p> <ul style="list-style-type: none"> <li>• Jenis</li> <li>• Versi</li> <li>• Diselenggara oleh pembekal/sendiri</li> </ul> <p>k) Adakah server tersebut dilengkapi oleh perisian antivirus? Jika YA, dapatkan maklumat antivirus tersebut :</p> <ul style="list-style-type: none"> <li>• Jenis</li> <li>• Kekurangan mengemaskini (<i>update</i>) <i>signature</i></li> <li>• Tarikh <i>virus signature</i> terkini</li> </ul>
4.0	<p><b>Tindakan Yang Diambil Oleh Agensi</b></p> <p>a) Boleh tuan/puan terangkan tindakan-tindakan yang telah dijalankan?</p> <p>b) Adakah server tersebut masih dihubungkan pada rangkaian? (Jika berkenaan)</p> <p>c) Adakah pihak tuan/puan mempunyai salinan imej (<i>backup</i>) data ke atas <i>server</i> yang diceroboh?</p> <p>i. Apakah bentuk media salinan (<i>backup</i>)</p> <p><i>Contoh:</i></p> <ul style="list-style-type: none"> <li>• <i>Hard disk</i> berasingan (<i>Separate hard disk</i>)</li> <li>• <i>Cartridge</i></li> <li>• <i>Optical Disk</i></li> <li>• <i>Imej backup</i></li> <li>• Lain-lain</li> </ul> <p><b>Nota:</b> Tujuan <i>backup</i> adalah untuk proses <i>restore</i> data selepas dibaikpulih</p> <p>d) Adakah terdapat <b>maklumat terperingkat</b> di dalam server tersebut?</p> <p>e) Adakah server di agensi tuan/puan pernah diceroboh/diserang sebelum ini? Jika YA, dapatkan maklumat lanjut.</p> <p>f) Adakah server tersebut telah dijalankan langkah-langkah pengukuhan (<i>patches</i>) sebelum ini? Jika YA,</p> <ol style="list-style-type: none"> <li>i. Dapatkan tarikh terakhir langkah-langkah pengukuhan dijalankan.</li> <li>ii. Apakah <i>patches</i> yang telah dilaksanakan?</li> </ol> <p>g) Apakah lain-lain tindakan yang telah diambil oleh agensi tuan/puan?</p> <p><i>Contoh:</i></p> <ol style="list-style-type: none"> <li>i. Melapor kepada GCERT/MyCERT</li> <li>ii. Melapor kepada Pembekal</li> <li>iii. Melapor kepada Pihak Penguatkuasa (PDRM)</li> </ol>

**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*, putus 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](mailto:cert@agensi.gov.my)) / ([cert\\_subagensi@agensi.gov.my](mailto:cert_subagensi@agensi.gov.my))

Cara mendapatkan fail log adalah seperti berikut:

**i. Win NT/Win 2000/Win 2003**

- **Web Access Log – Win NT/Win 2000**  
C:\WINNT\System32\Log Files
- **Web Access Log – Win 2003**  
C:\Windows\System32\Log Files
- **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](mailto:cert@agensi.gov.my)) / ([cert\\_subagensi@agensi.gov.my](mailto: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 analisis fail-fail log tersebut dan hasilnya akan dimajukan kepada pihak tuan/puan dengan kadar SEGERA (jika berkenaan).

	<p>c) Sekiranya berkenaan, tuan/puan disarankan untuk menjalankan langkah-langkah pengukuhan (<i>patches</i>). Boleh merujuk pada:</p> <ul style="list-style-type: none"> <li>• Laman web ICT Security (<a href="http://www.ictsecurity.gov.my">http://www.ictsecurity.gov.my</a>)</li> </ul> <p>d) Tuan/puan dinasihatkan supaya menjalankan salinan (<i>backup</i>) ke atas sistem yang diceroboh (sekiranya perlu)</p> <p>e) Tuan/puan juga dinasihatkan menjalankan pemeriksaan berikut ke atas server lain yang berada di dalam rangkaian yang sama (sekiranya perlu)</p> <p><i>Contoh:</i></p> <ul style="list-style-type: none"> <li>• Semak kandungan fail log</li> <li>• Semak <i>directory</i></li> <li>• Semak <i>temporary file</i></li> </ul> <p>f) i. Sebagai tindakan susulan, CERT Agensi memohon kerjasama tuan/puan untuk mengemukakan Borang Maklumat Pengendalian Insiden Keselamatan ICT iaitu Borang IRH 1.0</p> <p><b>Nota:</b></p> <p>Borang IRH 1.0 boleh diperolehi melalui laman web ICT Security pada URL <a href="http://agensi.gov.my">http://agensi.gov.my</a></p> <p>ii. Borang yang telah lengkap diisi bolehlah dikemukakan kepada CERT Agensi samada melalui e-mel CERT Agensi (<a href="mailto:cert@agensi.gov.my">cert@agensi.gov.my</a>)/(<a href="mailto:cert_subagensi@agensi.gov.my">cert_subagensi@agensi.gov.my</a>) atau melalui faks.</p> <p>g) (Jika berkenaan) Selepas fail-fail log diterima, CERT Agensi akan jalankan analisis fail-fail log tersebut dan hasilnya akan dimajukan kepada pihak tuan/puan SECEPAT MUNGKIN.</p> <p>h) Bolehkah tuan/puan maklumkan dengan SEGERA kepada CERT Agensi sekiranya semua langkah-langkah pengukuhan telah selesai supaya dapat dijalankan imbasan hos. Tujuannya adalah untuk menentukan tahap keselamatan server tersebut.</p> <p>i) Kemukakan laporan imbasan hos kepada agensi dan meminta agensi mengembalikan Borang IRH 1.1 – Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT.</p>
6.0	<p><b>PENUTUP</b></p> <p>a) Ucapkan terima kasih</p> <p>b) Minta kerjasama daripada agensi supaya mengikuti nasihat yang telah diberikan.</p> <p>c) Sekiranya mempunyai sebarang masalah/ memerlukan bantuan, minta agensi hubungi CERT Agensi di nombor dan email seperti berikut:</p> <ul style="list-style-type: none"> <li>i. Nombor Telefon: _____ (Pengurus CERT Agensi)</li> <li>ii. Nombor telefon Pegawai CERT Agensi yang mengendalikan insiden :</li> <li>iii. E-mel CERT Agensi : (<a href="mailto:cert@agensi.gov.my">cert@agensi.gov.my</a>)/(<a href="mailto:cert_subagensi@agensi.gov.my">cert_subagensi@agensi.gov.my</a>)</li> </ul>

Borang IRH 1.0 : Maklumat Pengendalian Insiden Keselamatan ICT

SULIT



**Borang IRH 1.0 - Maklumat Pengendalian Insiden  
Keselamatan ICT**

Tarikh dan Masa :  
Pengendalian

<b>Computer Emergency Response Team Agensi (CERT Agensi)</b>	
*No. Insiden	Tahun/Bulan/Kod Kategori/Bil insiden dalam tahun semasa  (Diisi oleh CERT Agensi)
*Tarikh & Masa Dikesan	(Diisi oleh CERT Agensi)
<b>Maklumat Organisasi/Agensi</b>	
ICTSO 1. Nama 2. Jawatan dan Gred 3. No. Telefon Pejabat 4. No. Telefon Bimbit 5. E-mel	
Pentadbir Sistem 1. Nama 6. Jawatan dan Gred 7. No. Telefon Pejabat 8. No. Telefon Bimbit 2. E-mel	
Pegawai Perhubungan 1. Nama 9. Jawatan dan Gred 10. No. Telefon Pejabat 11. No. Telefon Bimbit 2. E-mel	
Alamat Penuh Agensi	
Bahagian/Unit Yang Melapor	
No. Telefon Agensi	
No. Faks	
<b>Maklumat Perkakasan dan Perisian Yang Terlibat</b>	
Hostname	
Domain	
DNS	
Alamat IP 1. Internal 2. External	
Sistem Pengoperasian 1. Jenis 2. Versi 3. Service pack	

Kapasiti Disk
Jenis <i>Hard Disk</i>
Sistem Aplikasi/Perkhidmatan lain
<b>Maklumat Insiden</b>
Alamat IP Penyerang
Jenis Insiden <span style="float: right;">e.g. unauthorized access, malicious code</span>
Jenis Serangan
<b>Tindakan Yang Diambil Oleh CERT Agensi</b>
<b>(Diisi oleh CERT Agensi)</b>

**Computer Emergency Response Team (CERT) Agensi**  
**Alamat CERT Agensi**  
**Email CERT Agensi**



**Keterangan Lanjut Mengenai Insiden**

(Nyatakan tarikh, masa, tempoh tindakan pengukuhan, jenis kerosakan, kesan ke atas maklumat atau sistem dan lain-lain maklumat yang dikira relevan sekiranya diketahui.)

Tarikh dan Masa/ : Tempoh Tindakan Pengukuhan	
Jenis Kerosakan :	
Kesan Ke Atas : Maklumat/Sistem	
Perkakasan ICT : Yang Terlibat & Bil.	
Khidmat Teknikal : Yang Terlibat Dalam Baikpulih/ Pengukuhan	<input type="checkbox"/> Pembekal <input type="checkbox"/> Dalaman – Bil. .... orang Lain-Lain : .....
Kos Baikpulih :	RM

**Pelaksanaan Pengukuhan Oleh:**

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

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

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

**Computer Emergency Response Team (CERT) Agensi  
Alamat CERT Agensi  
Email CERT Agensi**

**SULIT**

SULIT

LAPORAN ANALISIS FAIL LOG

Nama Agensi :  
 Nama Fail Log :  
 No. Insiden :

Bil.	Alamat IP Penyerang	Masa	Aktiviti
1.	Senaraikan alamat IP penyerang	Catatkan masa yang terlibat	Senaraikan jenis <i>vulnerability</i> yang ada dan <i>script</i> yang terlibat (dalam fail log)
2.			
3.			

Rujukan Fail CERT Agensi-Tarikh

SULIT



**SULIT**

**LAPORAN IMBASAN HOS**

**Nama Agensi** :  
**Alamat IP** :  
**Julat IP** :  
**URL** :

**1. Penemuan**

**2. Rumusan**

Rujukan Fail CERT Agensi-Tarikh

**SULIT**

SULIT

LAPORAN KRONOLOGI INSIDEN KESELAMATAN ICT

Nama Agensi :

Tarikh :

Lokasi :

TARIKH	MASA	AKTIVITI	HASIL SIASATAN/PENEMUAN

Rujukan Fail CERT Agensi-Tarikh

SULIT

## SINGKATAN PERKATAAN

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