PROSEDUR PENGENDALIAN INSIDEN KESELAMATAN ICT

MS ISO/IEC 27001:2013

KEMENTERIAN PENGAJIAN TINGGI

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
Nama : EMELIA MARDIANA BINTI SAMSI Jawatan : Penolong Setiausaha Kanan Bahagian Pengurusan Maklumat Kementerian Pengajian Tinggi Tarikh:	Nama : RANI BINTI ARIS @ AZIS Jawatan: Ketua Penolong Setiausaha Bahagian Pengurusan Maklumat Kementerian Pengajian Tinggi Tarikh :	Nama : ABDULLAH BIN JAMIL Jawatan: Ketua Penolong Setiausaha Kanan Bahagian Pengurusan Maklumat Kementerian Pengajian Tinggi Tarikh : 22/02/2021

REKOD PINDAAN DOKUMEN

TARIKH	NO. KELUARAN/PINDAAN	BAB/MUKA SURAT	KETERANGAN PINDAAN
07/12/2017	1.0		
22/02/2021	1.1	Keseluruhan dokumen	Menggantikan tanggungjawab MAMPU kepada NACSA
		m/9	Kemaskini keahlian CERT KPT
		m/s 17	Tambahan lampiran C,D & E

PROSEDUR PENGENDALIAN INSIDEN KESELAMATAN ICT

KANDUNGAN

1.0 TUJUAN 4
2.0 LATAR BELAKANG 4
3.0 PROSES AM BAGI PENGENDALIAN INSIDEN DI KPT 5
4.0 TAHAP KEUTAMAAN TINDAKAN KE ATAS INSIDEN 8
5.0 PENUBUHAN CERT AGENSI 9
6.0 TANGGUNGJAWAB CERT AGENSI 10
7.0 PROSES PELAPORAN INSIDEN KESELAMATAN ICT 12
8.0 PROSES KERJA / TINDAKAN 15
9.0 REKOD 17
10.0 LAMPIRAN 17

1.0 TUJUAN

Prosedur ini bertujuan untuk membantu *Computer Emergency Response Team* (CERT) Kementerian Pengajian Tinggi (KPT) di dalam mengurus pelaporan dan pengendalian insiden keselamatan ICT di KPT dan agensi di bawah kawalannya.

2.0 LATAR BELAKANG

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.

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.

Agensi Keselamatan Siber Negara (NACSA) di bawah Majlis Keselamatan Negara, Jabatan Perdana Menteri telah ditubuhkan pada 1 Februari 2017 sebagai agensi peneraju dalam bidang keselamatan siber negara yang bertanggungjawab menangani ancaman siber termasuk memantau dan menyelaras tindakan bagi melindungi aset kritikal negara. Selaras dengan penubuhan NACSA, fungsi pengurusan pengendalian GCERT oleh MAMPU kini telah dipertanggungjawabkan kepada NACSA bermula pada 1 Januari 2018. Fungsi pengurusan pengendalian insiden keselamatan ICT perlu dilaksanakan selari dengan fungsi-fungsi NACSA yang lain. (Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency

Response Team (GCERT) oleh Agensi Keselamatan Siber Negara (NACSA) bertarikh 28 Januari 2019).

3.0 PROSES AM BAGI PENGENDALIAN INSIDEN DI KPT

Pengendalian insiden di KPT terbahagi kepada dua (2) kategori:

a) Kategori 1 : Insiden Keselamatan ICT

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:

i. Dasar Keselamatan ICT KPT Pelanggaran Dasar (Violation of Policy)
Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Dasar Keselamatan ICT.

ii. 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.

iii. 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.

iv. 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).

v. 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.

vi. 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.

vii. Harrassment/Threats

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

viii. 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.

ix. Kehilangan Fizikal (Physical Loss)

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

Rujuk pada Lampiran 1 dan Lampiran 2 bagi proses pelaporan bagi insiden keselamatan ICT sektor awam.

b) Kategori 2 : Insiden Dalaman Pusat Data

Insiden Pusat Data adalah insiden yang berkaitan dengan jenis kerosakan yang berlaku ke atas aset fizikal Pusat Data yang tidak melibatkan gangguan terhadap pengoperasian di Pusat Data secara terus. Contoh insiden Pusat Data adalah seperti kerosakan pada pintu, kerosakan pada lampu, kerosakan pada penghawa dingin, penggera alarm keselamatan tidak berfungsi, kerosakan pada siling dan bumbung, CCTV tidak berfungsi, tingkap pecah, dinding retak dan kerosakan fizikal yang lain. Pelaporan dan pengendalian bagi insiden dalaman di Pusat Data boleh dilakukan menggunakan Laporan Penambahbaikan dan Pembetulan (KPT-BPM-ISMS-P1-010-01) pada Lampiran 1 dalam Prosedur Tindakan Penambahbaikan dan Pembetulan dan Borang Permohonan Perubahan (KPT-BPM-ISMS-P3-004-02) pada Lampiran 2 jika melibatkan sebarang perubahan berkaitan.

4.0 TAHAP KEUTAMAAN TINDAKAN KE ATAS INSIDEN

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

a) Keutamaan 1 (Merah)

Insiden keselamatan ICT yang membawa ancaman nyawa, menggugat keselamatan dan pertahanan negara, menjejas ekonomi dan imej negara, yang mungkin memerlukan Pelan Pemulihan Perkhidmatan (BCP) diaktifkan.

b) Keutamaan 2 (Kuning)

Insiden keselamatan ICT selainnya seperti pencerobohan laman web, gangguan sistem dan pencerobohan aset ICT.

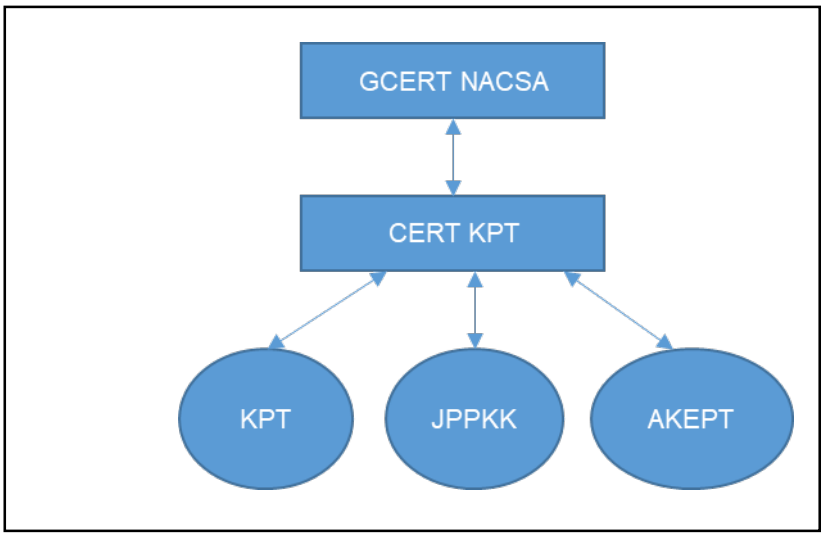
c) Keutamaan 3 (Biru)

Insiden keselamatan yang berskala kecil seperti kerosakan perkakasan/perisian ICT samada di dalam Pusat Data atau ruang kerja, kehilangan peralatan ICT (yang tidak melibatkan maklumat sensitif), ancaman virus/malware berskala kecil yang tidak menyebabkan gangguan dan kebocoran penghawa dingin.

5.0 PENUBUHAN CERT AGENSI

Model struktur pasukan CERT KPT adalah berdasarkan Model 1 seperti mana yang dicadangkan di dalam garis panduan yang dikeluarkan. Menerusi model ini, satu pasukan pengendali insiden ditubuhkan dan bertanggungjawab mengenai pengurusan insiden di agensi-agensi atau bahagian di bawah kawalannya.

Model Pasukan CERT KPT adalah seperti di bawah:



Rajah 1- Model CERT KPT

Wakil keahlian di CERT KPT adalah seperti berikut:

Bil.	Jawatan	Peranan
1.	CIO KPT	Pengarah CERT KPT
3.	ICTSO KPT	Pengurus CERT KPT
4.	KPSUK(M)PA	Ahli CERT KPT
5.	KPSUK(M)DL	Ahli CERT KPT
6.	PSUK(M)TR3	Ahli CERT KPT
7.	PSUK(M)TD	Ahli CERT KPT
8.	PPTMK(M)TR	Ahli CERT KPT
9.	ICTSO JPPKK	Ahli CERT KPT
10.	Wakil AKEPT	Ahli CERT KPT

6.0 TANGGUNGJAWAB CERT AGENSI

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

a) Menerima dan mengesan aduan keselamatan ICT serta 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 Agensi Keselamatan Siber Negara (NACSA) sama ada sebagai input atau untuk tindakan seterusnya;
e) Menasihat agensi-agensi di bawah KPT mengambil tindakan pemulihan dan pengukuhan;
f) Menyebarkan makluman berkaitan pemulihan dan pengukuhan kepada semua pengguna KPT; dan
g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baharu dapat dielakkan.

Apabila berlaku insiden, ICTSO perlu menilai risiko kerumitan insiden yang berlaku dan menentukan tahap kerumitan insiden. Bagi insiden yang dinilai berada di dalam kategori tahap keutamaan 1 (Merah), insiden perlu dimaklumkan kepada CIO, CERT KPT dan NACSA. Manakala kategori tahap keutamaan 2 (Kuning) insiden perlu dimaklumkan kepada CERT KPT dan NACSA.

Pengarah CERT KPT perlu menggerakkan ahli CERT KPT untuk mengambil tindakan berikut:

a) Mengurus dan mengambil tindakan ke atas insiden yang berlaku sehingga keadaan pulih; dan
b) Menentukan samada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang/keselamatan.

Sekiranya insiden yang dinilai berada di dalam tahap keutamaan 3 (Biru), insiden tersebut hanya perlu diselesaikan di peringkat dalaman BPM atau makluman kepada ICTSO sahaja. Laporan lengkap insiden yang berlaku juga perlu direkodkan.

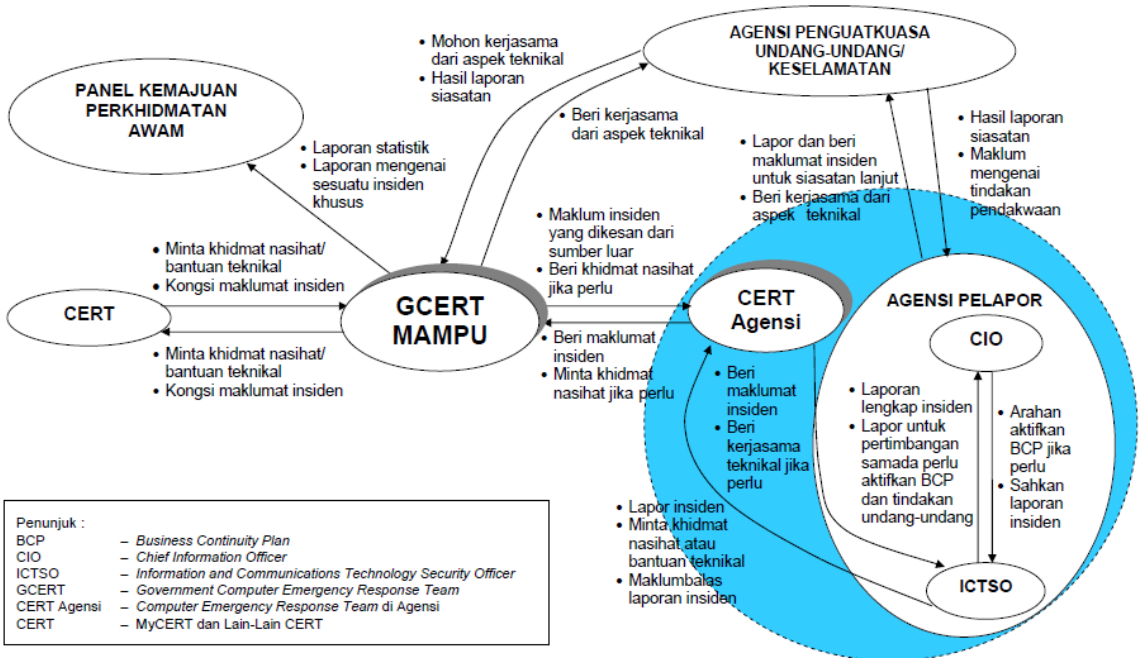
Jadual di bawah merumuskan tahap proses pelaporan sesuatu insiden:

Bil.	Tahap Insiden	Tahap Pelaporan
1.	Keutamaan 1 (Merah)	Pelapor → ICTSO KPT → CIO → CERT KPT → GCERT
2.	Keutamaan 2 (Kuning)	Pelapor → ICTSO KPT → CIO → CERT KPT → GCERT
3.	Keutamaan 3 (Biru)	Pelapor → ICTSO KPT (jika perlu)

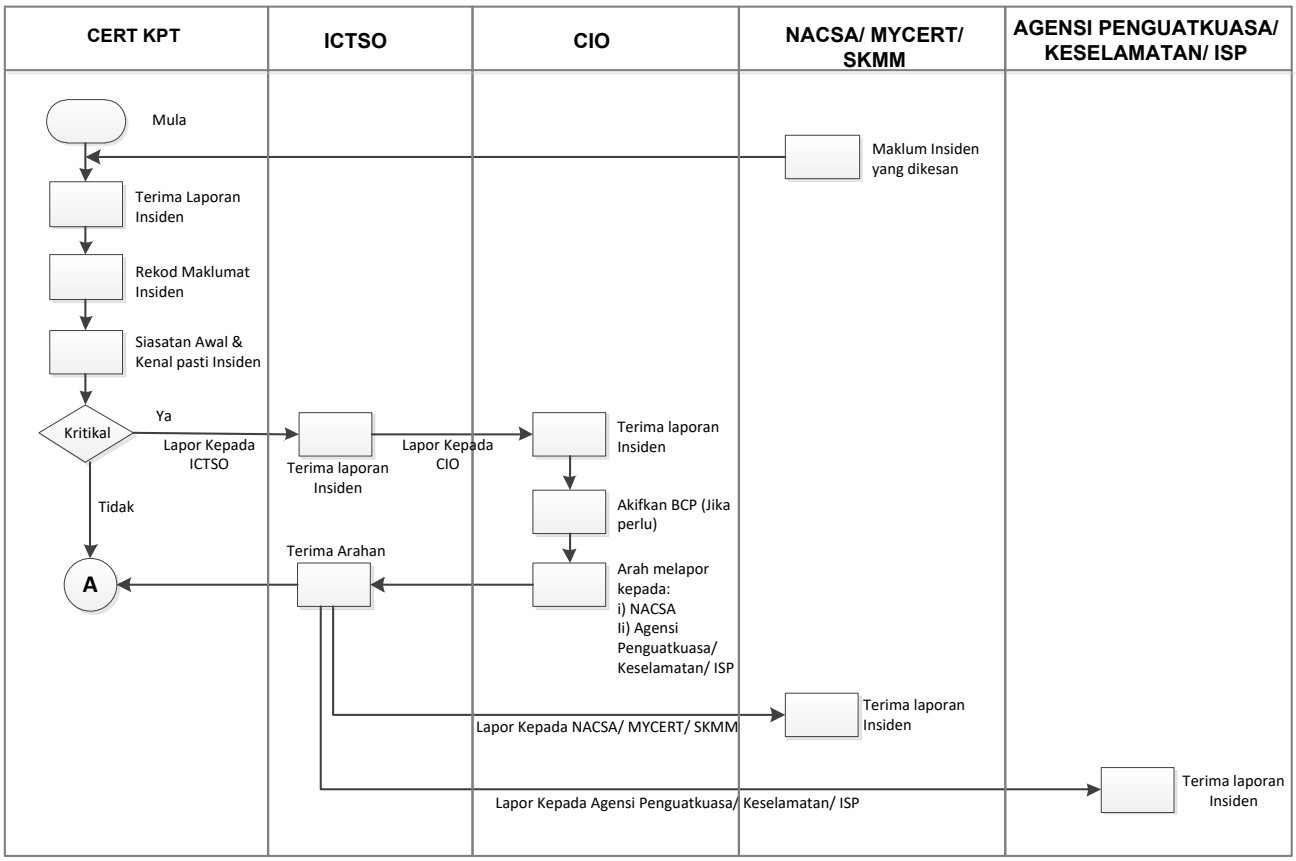
7.0 PROSES PELAPORAN INSIDEN KESELAMATAN ICT

Proses Pelaporan Insiden Keselamatan ICT diringkaskan dalam Rajah 2 – Hubungan Entiti Dalam Proses Kerja Pelaporan Insiden Keselamatan ICT dan carta aliran di bawah.

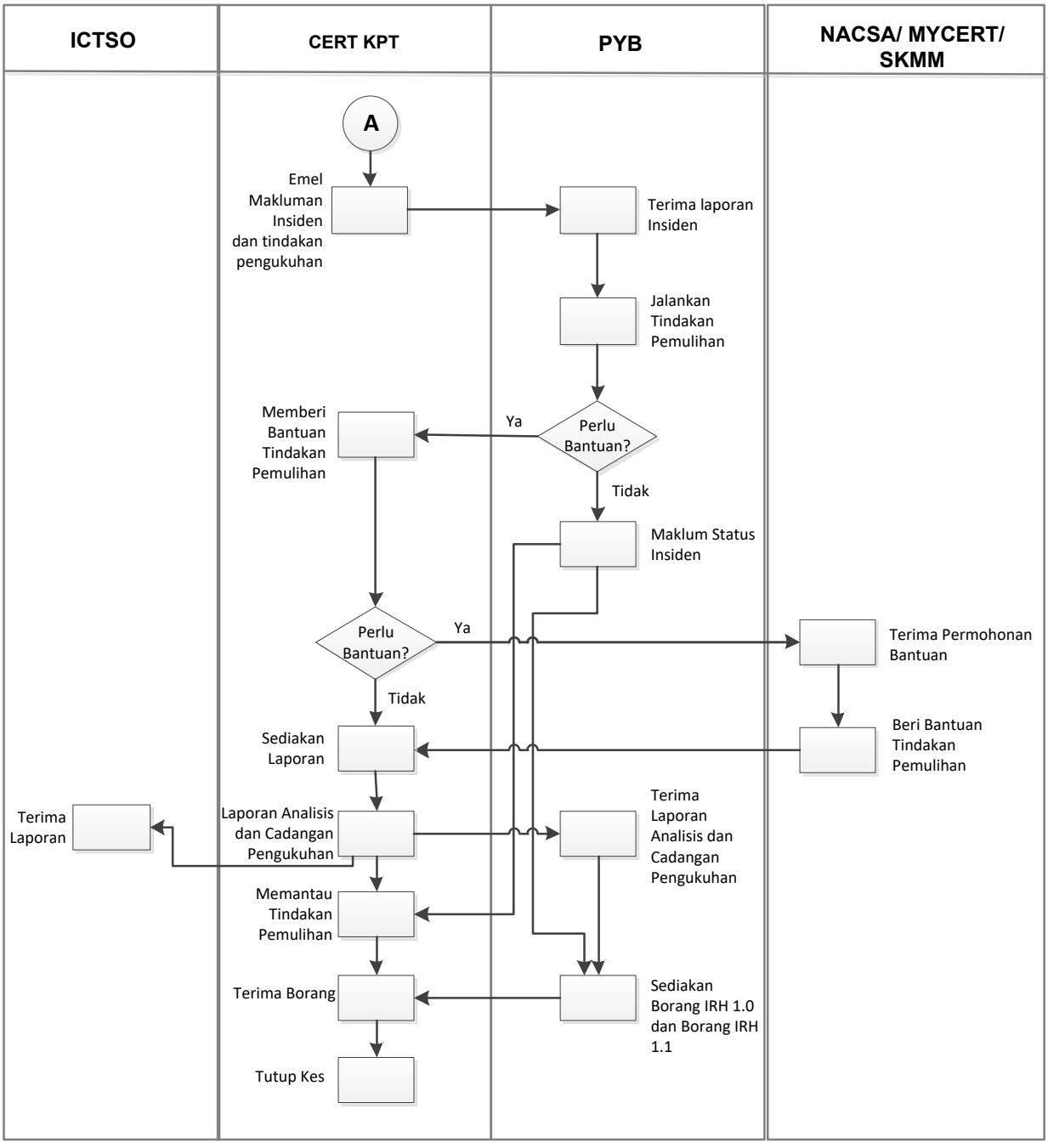
Rajah 2: Hubungan Entiti dalam Proses Kerja Pengurusan Pelaporan Insiden Keselamatan ICT.



7.1 Proses Pelaporan Insiden Keselamatan ICT



7.2 Proses Pengendalian Insiden Keselamatan ICT



8.0 PROSES KERJA / TINDAKAN

8.1 Proses Pelaporan Insiden Keselamatan ICT

PROSES KERJA	TANGGUNGJAWAB
9.1.1 Terima laporan insiden daripada NASCA, MyCERT, SKMM atau dalaman KPT melalui e-mel.	CERT KPT
9.1.2 Rekod insiden yang diterima di dalam fail insiden dan Borang IRH 1.0 - Maklumat Pengendalian Insiden Keselamatan ICT.	CERT KPT
9.1.3 Jalankan kajian/siasatan awal ke atas insiden.	CERT KPT
9.1.4 Maklum insiden kepada ICTSO.	CERT KPT
9.1.5 Tentukan jenis insiden dan tahap keutamaan tindakan ke atas insiden.	ICTSO
9.1.6 Jika tahap keutamaan insiden 1 (Merah): i. ICTSO maklum insiden kepada CIO. ii. CIO mengarahkan untuk mengaktifkan Pelan Pemulihan Perkhidmatan (BCP) jika perlu. iii. CIO mengarahkan lapor insiden kepada NACSA dan Agensi Penguatkuasa/ Keselamatan / ISP	CIO ICTSO
9.1.7 Jika tahap keutamaan insiden 2 (Kuning): i. Maklum insiden kepada ICTSO dan NACSA.	CERT KPT

8.2 Proses Pengendalian Insiden Keselamatan ICT

PROSES KERJA	TANGGUNGJAWAB
11.2.1 Hantar e-mel makluman insiden dan tindakan pengukuhan bersama borang IRH 1.0 dan 1.1 kepada pegawai yang bertanggungjawab.	CERT KPT
11.2.2 Terima laporan insiden daripada CERT KPT melalui e-mel.	PYB
11.2.3 Jalankan tindakan pemulihan	PYB

PROSES KERJA	TANGGUNGJAWAB
11.2.4 Sekiranya PYB perlu bantuan CERT KPT: i. Hantar permohonan bantuan dan fail log untuk dianalisis kepada CERT KPM. ii. Terima laporan analisis dan cadangan tindakan pengukuhan daripada CERT KPT.	PYB
11.2.5 Sekiranya CERT KPT perlu bantuan NACSA: i. Hantar permohonan bantuan dan fail log untuk dianalisis kepada NACSA/MYCERT/SKMM. ii. Terima laporan analisis dan cadangan tindakan pengukuhan daripada NACSA/MYCERT/SKMM.	CERT KPT
11.2.6 Hantar laporan analisis dan cadangan tindakan pengukuhan kepada pegawai yang bertanggungjawab terhadap insiden.	CERT KPT
11.2.7 Pantau pelaksanaan tindakan pemulihan oleh pegawai yang bertanggungjawab terhadap insiden.	CERT KPT
11.2.8 Hantar Borang IRH 1.0 dan Borang IRH 1.1 yang telah dilengkapkan kepada CERT KPT.	PYB
11.2.9 Kemaskini statistik insiden dan masukkan dalam fail Insiden.	CERT KPT

9.0 REKOD

BIL	TAJUK	LOKASI	TANGGUNG JAWAB	TEMPOH SIMPANAN
1	Fail Insiden	Bilik Fail	PYB	5 Tahun
2	Borang IRH 1.0 - Maklumat Pengendalian Insiden Keselamatan ICT	Bilik Fail	PYB	5 Tahun
3	Borang IRH 1.1 - Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT	Bilik Fail	PYB	5 Tahun

10.0 LAMPIRAN

- Lampiran A : Borang IRH 1.0
- Lampiran B : Borang IRH 1.1
- Lampiran C : Template Laporan Analsis Fail Log
- Lampiran D : Template Laporan Imbasan Hos
- Lampiran E : Template Laporan Kronologi Insiden Keselamatan ICT

Lampiran A

SULIT

Kementerian Pengajian Tinggi

Borang IRH 1.0 - Maklumat Pengendalian Insiden Keselamatan ICT

Tarikh dan Masa : Pengendalian

Computer Emergency Response Team Agensi (CERT KPT)	
*No. Insiden	Tahun/Bulan/Kod Kategori/Bil insiden dalam tahun semasa **(Diisi oleh CERT KPT)**
*Tarikh & Masa Dikesan	**(Diisi oleh CERT KPT)**
Maklumat Organisasi/Agensi	
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	
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
Tindakan Yang Diambil Oleh CERT KPT
(Diisi oleh CERT KPT)

Computer Emergency Response Team (CERT)
Kementerian Pengajian Tinggi
Bahagian Pengurusan Maklumat
Aras 6, No. 2, Menara 2, Jalan P5/6, Presint 5
62200 W.P. Putrajaya
Tel: 0388706061
Faks: 0388706819

certkpt@mohe.gov.my

SULIT

Lampiran B

SULIT

Kementerian Pengajian Tinggi

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

No. Insiden :

Kepada:

Pengarah
Alamat CERT Agensi

Merujuk kepada Laporan Imbasan Hos/serangan *malicious code* bertarikh _____ adalah dimaklumkan tindakan pengukuhan keselamatan ICT* **TELAH/BELUM** dijalankan sebagaimana yang telah dicadangkan.
(* Potong yang tidak berkenaan)

Sila jelaskan tindakan yang **TELAH** diambil atau nyatakan sebab jika **BELUM**

_____

_____

_____

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	Pembekal 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 :

SULIT

Lampiran C

SULIT

LAPORAN ANALSIS 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 *vulnerability* yang ada dan *script* yang terlibat (dalam fail log)**
2.			
3.			

Rujukan Fail CERT Agensi-Tarikh

SULIT

Lampiran D

SULIT

LAPORAN IMBASAN HOS

Nama Agensi :
Alamat IP :
Julat IP :
URL :

1. Penemuan

2. Rumusan

Rujukan Fail CERT Agensi-Tarikh

SULIT

Lampiran E

SULIT

LAPORAN KRONOLOGI INSIDEN KESELAMATAN ICT

Nama Agensi :

Tarikh :

Lokasi :

TARIKH	MASA	AKTIVITI	HASIL SIASATAN/PENEMUAN

Rujukan Fail CERT Agensi-Tarikh

SULIT