(4)

SURAT PEKELILING ICT NO. 3/2009

DARIPADA: Setiausaha Kerajaan Negeri

KEPADA: Semua Setiausaha Tetap Kementerian Negeri
Semua Ketua Jabatan Negeri
Semua Residen dan Pegawai Daerah
Semua Ketua Badan Berkanun Negeri
Semua Pihak Berkuasa Tempatan

PERKARA: Penubuhan QCERT Dan Pengurusan Pengendalian Insiden ICT Sektor Awam di Peringkat Negeri

RUJ. KAMI: JKM/ICT/ADM04/004V.1 (41) **TARIKH:** 5 November 2009

TUJUAN

Surat Pekeliling ini bertujuan memperkemaskan pengurusan pengendalian insiden keselamatan ICT bagi sektor awam di Peringkat Negeri supaya sebarang kejadian insiden keselamatan ICT dapat diuruskan dengan segera dan sistematik di mana kesannya dapat diminimumkan dan penyebarannya ke agensi lain dapat dibendung.

2. Kerajaan Negeri memandang berat tentang isu-isu keselamatan ICT dalam pelaksanaan Kerajaan Elektronik sebagai salah satu usaha dalam mempertingkatkan penyampaian perkhidmatan kepada rakyat. Peningkatan jenayah siber masa kini memberi kesan dan impak yang serius dalam keselamatan maklumat dan asset-asset ICT di agensi-agensi Kerajaan. Oleh yang demikian, Kerajaan memberi perhatian serius terhadap isu keselamatan ICT bagi memastikan agensi Kerajaan terus beroperasi dengan lancar.

3. Surat Pekeliling ini adalah selaras dengan seruan Kerajaan Pusat melalui Pekeliling Am Bil. 4 Tahun 2006: "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat (ICT) Sektor Awam", di mana MAMPU menyeru Kerajaan Negeri untuk menubuhkan pasukan CERT di agensi Kerajaan untuk memperkukuh dan melancarkan lagi pengurusan insiden ICT di peringkat Negeri.

LATARBELAKANG

4. Sehubungan itu, Kerajaan Negeri telah menubuhkan pasukan CERT yang dikenali sebagai **Sarawak Computer Emergency Response Team (QCERT)**. QCERT bertindak memberi *first level support* dalam menangani insiden ICT yang berlaku di agensi-agensi Kerajaan Negeri, sebelum dilaporkan di Peringkat Kerajaan Pusat.

copy

5. QCERT adalah hakmilik penuh Kerajaan Negeri Sarawak, di mana pasukan ini akan diketuai oleh Unit ICT, Jabatan Ketua Menteri Negeri Sarawak.

INSIDEN KESELAMATAN ICT

6. Insiden keselamatan bermaksud musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi (ICT) atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT samada yang ditetapkan secara tersurat atau tersirat.

7. Jenis insiden dapat dikenalpasti seperti berikut:

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

Penggunaan asset 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 identity yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identity, 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 asset ICT berpunca dari ancaman pencerobohan.

TAHAP KEUTAMAAN TINDAKAN KE ATAS INSIDEN

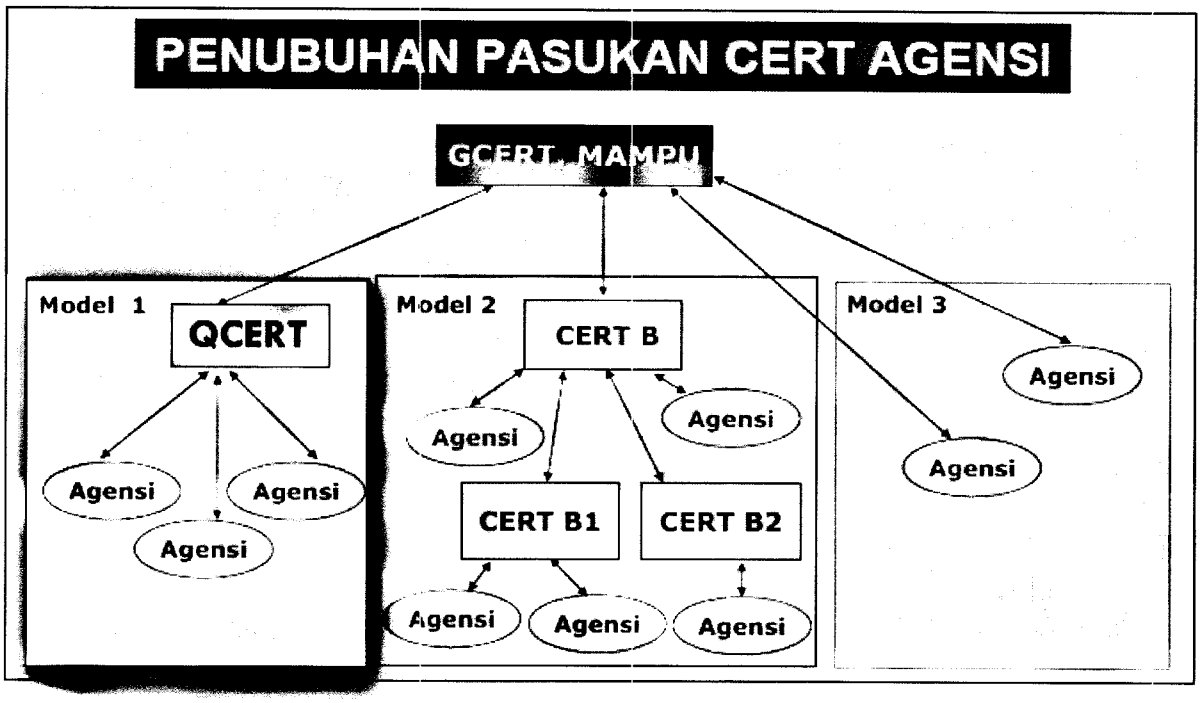
8. Tindakan ke atas insiden yang berlaku hendaklah dibuat berasaskan kepada keparahan sesuatu insiden. Tahap keutamaan tindakan ke atas insiden akan ditentukan seperti berikut:

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

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

PENUBUHAN QCERT

9. Struktur pasukan QCERT adalah seperti Model 1 yang dicadangkan di gambarajah 1.



Gambarajah 1 : Model Pasukan CERT Sarawak (QCERT)

10. Keahlian QCERT adalah seperti berikut:

(a)	Pengarah QCERT	: Pengarah Unit ICT, Jabatan Ketua Menteri (Pegawai CIO Negeri)
(b)	Pengurus QCERT	: Ketua Penolong Pengarah, Seksyen Kerajaan Elektronik, Unit ICT, Jabatan Ketua Menteri (Pegawai ICTSO Negeri)
(c)	Ahli	: 1) Ketua Penolong Pengarah, Seksyen Perancangan dan Perlaksanaan Teknologi Maklumat, Unit ICT, Jabatan Ketua Menteri. (Pegawai CIO, Unit ICT)

2) Pegawai ICTSO, Unit ICT,
Jabatan Ketua Menteri
(Pegawai ICTSO, Unit ICT)

3) Pegawai sistem perisian, Unit ICT
4) Pegawai sistem rangkaian, Unit ICT
5) Pegawai fail log, Unit ICT
6) Ketua Penolong Pengarah,
Unit Audit Dalam, Jabatan Ketua Menteri
7) Pegawai ICTSO, Unit Keselamatan,
Jabatan Ketua Menteri

TANGGUNGJAWAB QCERT

11. Ia bertanggungjawab menangani semua laporan insiden keselamatan ICT yang melibatkan sektor awam di Negeri Sarawak. Secara amnya tugas QCERT adalah seperti berikut:

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

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

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

(d) Melaporkan insiden kepada pihak Kerajaan Pusat, *Government Computer Emergency Response Team (GCERT),* MAMPU.

PROSES PELAPORAN INSIDEN PERINGKAT NEGERI

12. Ketua Jabatan hendaklah memainkan peranan penting bagi memastikan agensi mematuhi arahan mengenai pengurusan insiden di agensi di bawah kawalan masing-masing. Ketua Jabatan juga hendaklah memastikan jabatan dan agensi di bawah kawalannya meningkatkan pematuhan ke atas kehendak akta, arahan, peraturan dan prosedur berkaitan keselamatan ICT yang telah dikeluarkan oleh Kerajaan Negeri seperti:

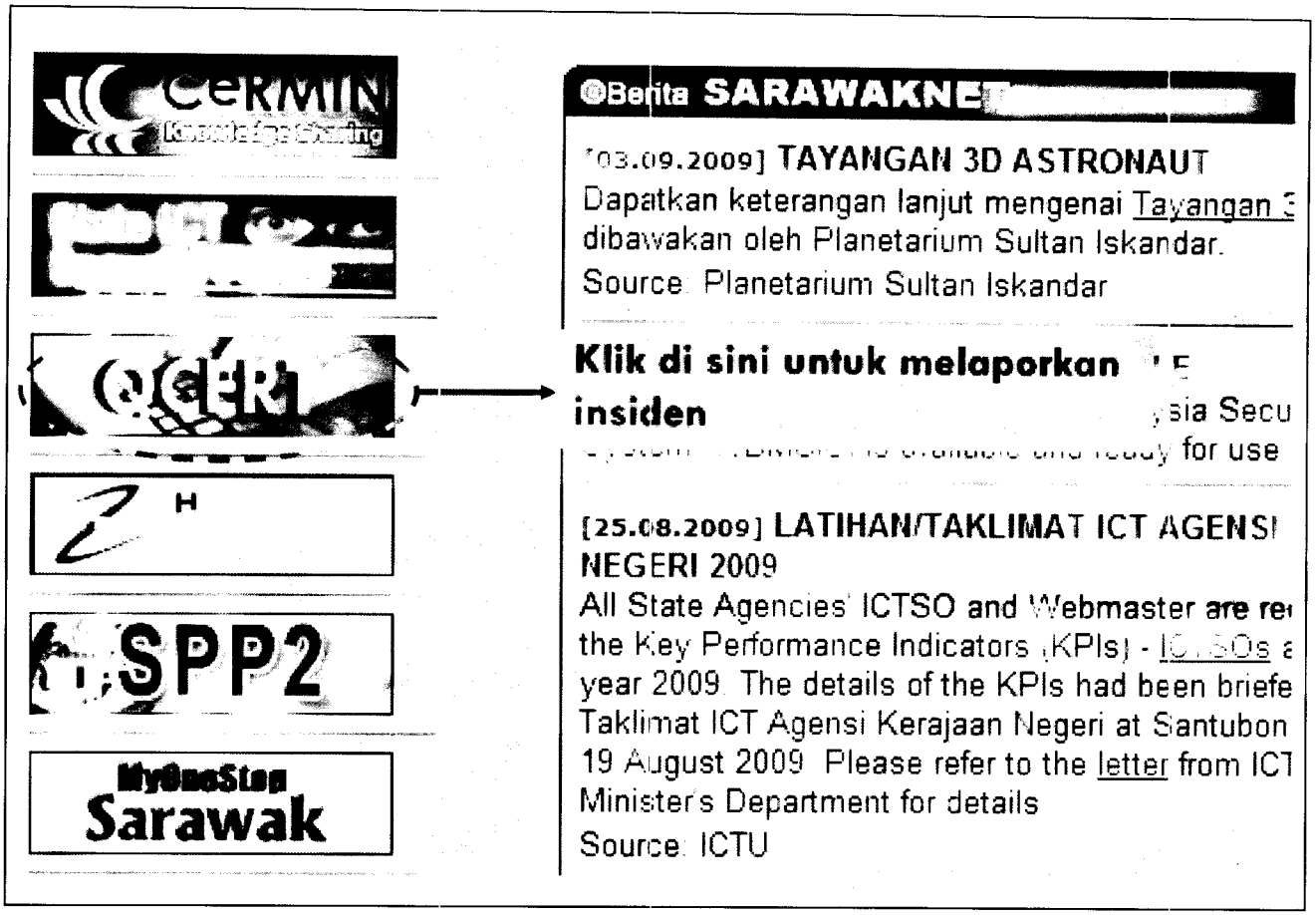
a. Polisi *Desktop Security Management* (DSM) – Surat Pekeliling No. 1/2006

b. Polisi *Network Security Management* (NSM) – Surat Pekeliling ICT No.5/2008

13. Proses pelaporan dijelaskan di Lampiran A. Lampiran A1 menunjukkan hubungan antara agensi dan entiti yang terlibat dalam proses pelaporan manakala

Lampiran A2 merupakan aliran kerja terperinci bagi proses pelaporan insiden keselamatan ICT sektor awam.

14. Laporan insiden dibuat oleh Pegawai Keselamatan ICT (ICTSO) agensi secara dalam talian di QCERT portal melalui laman utama SarawakNet (www.sarawaknet.gov.my) dengan mengklik ikon QCERT yang terdapat di sebelah kiri laman web. Sila rujuk gambarajah seperti di bawah:



15. Pihak QCERT juga boleh dihubungi melalui kaedah-kaedah seperti berikut:

Email	: qcert@sarawaknet.gov.my
Telephone	: 555999 (seluruh Negeri)
Handphone	: 082-555999 (seluruh Negeri)
Fax	: 555888 (seluruh Negeri)

Adalah dimaklumkan bahawa nombor talian QCERT adalah sama dengan nombor Talikhidmat.

16. Sekiranya terdapat sebarang kemusykilan berkaitan dengan Surat Pekeliling ini, sila rujuk kepada Unit ICT, Jabatan Ketua Menteri di talian **082-492851** atau email: **qcert@sarawaknet.gov.my.**

TARIKH KUATKUASA

17. Surat Pekeliling ini berkuatkuasa dengan serta-merta.

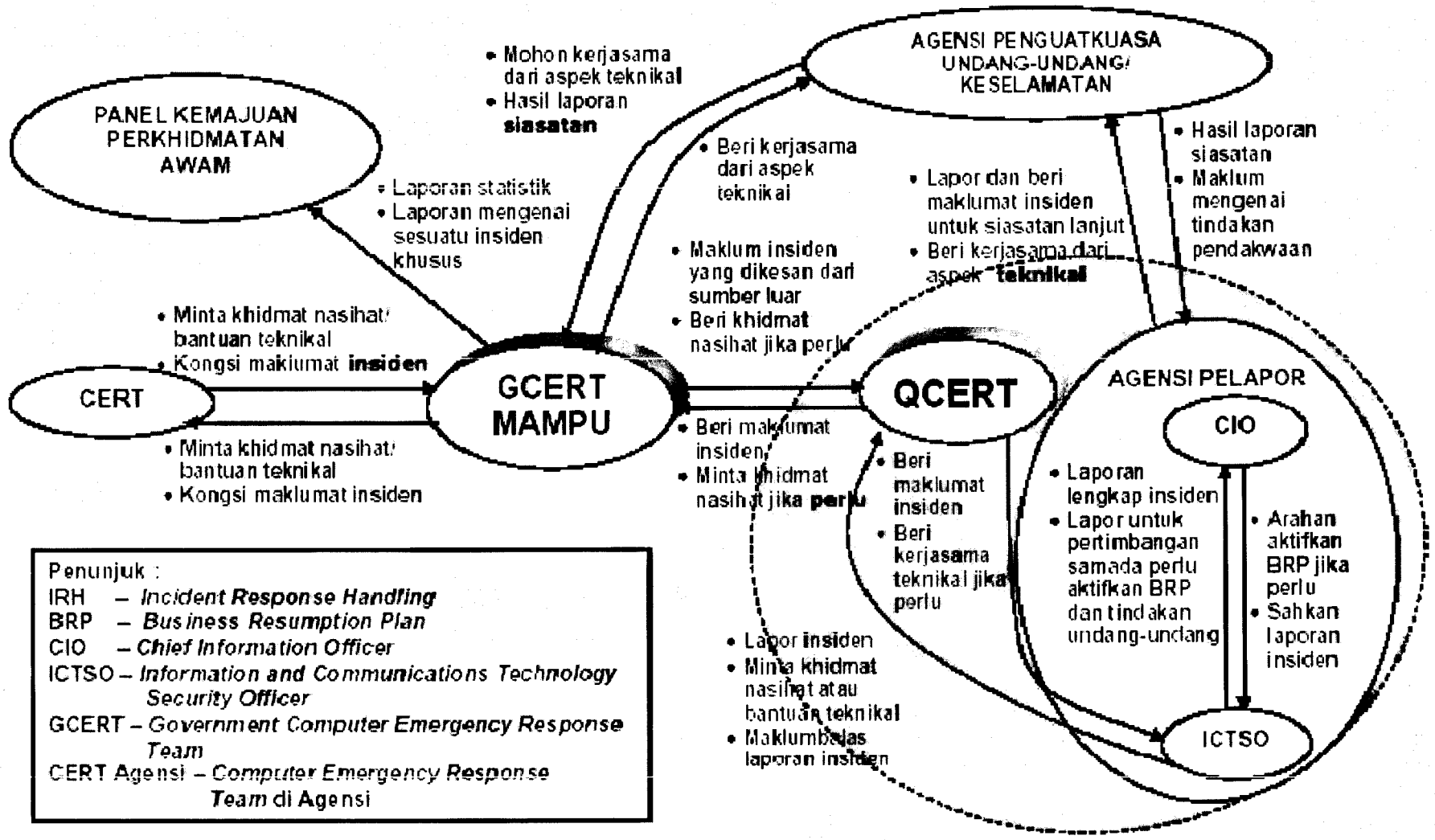
Sekian, harap maklum.

"BERSATU BERUSAHA BERBAKTI"

"AN HONOUR TO SERVE"

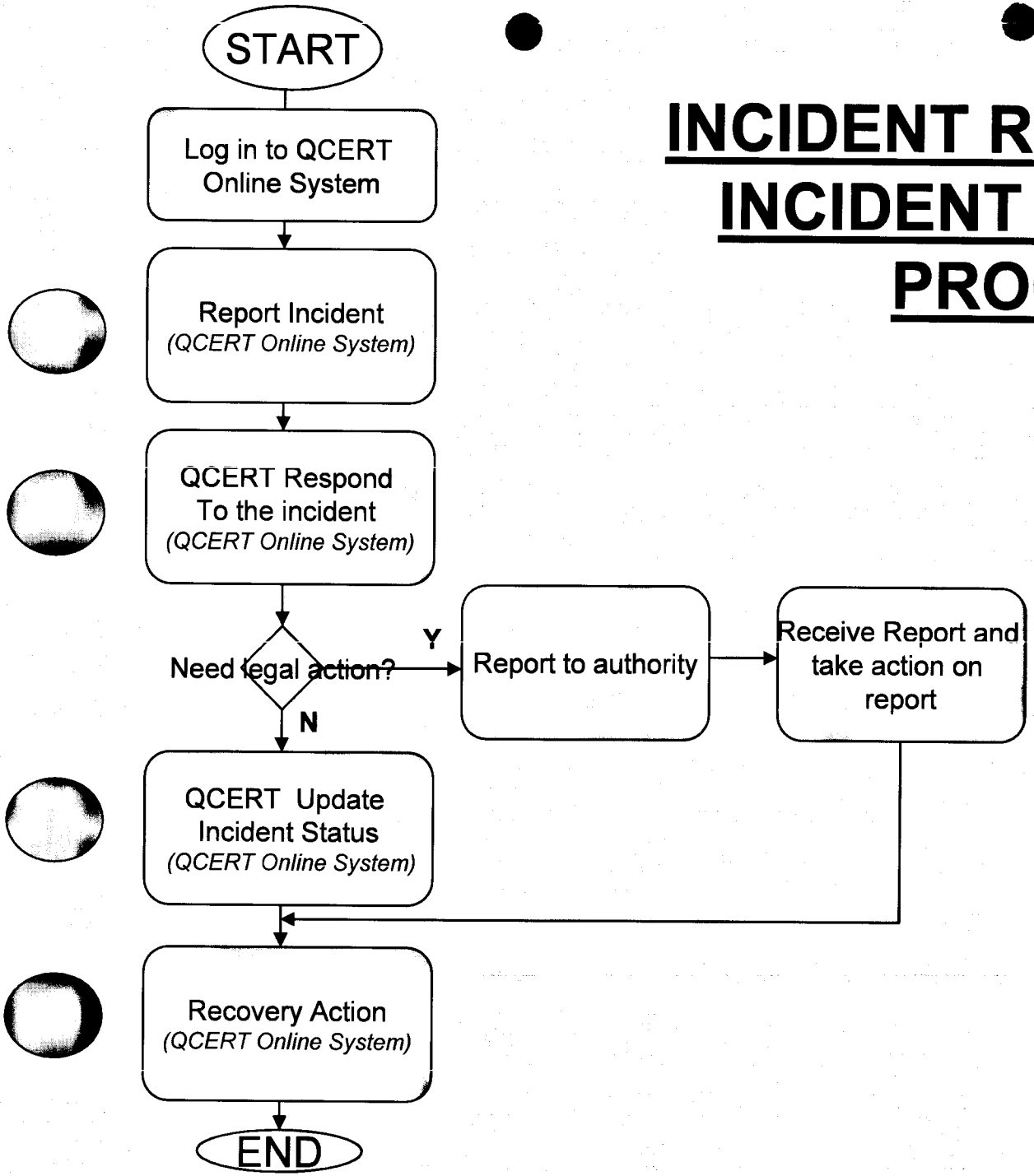
(DATUK AMAR HAJI MOHAMAD MORSHIDI BIN ABDUL GHANI)
Setiausaha Kerajaan Negeri
Sarawak

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

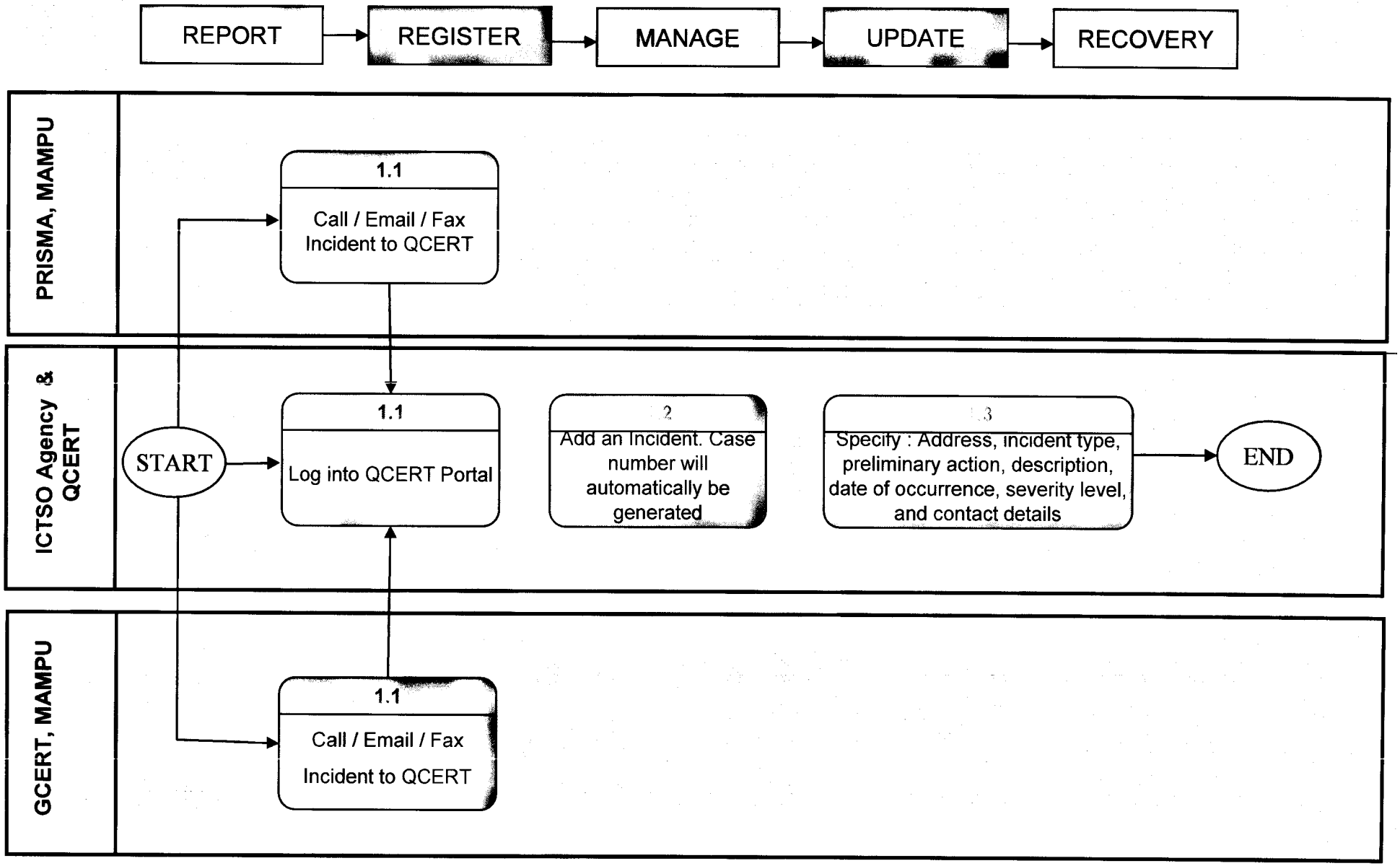


LAMPIRAN A2

INCIDENT REPORTING & INCIDENT HANDLING PROCESS



Reporting a Security Incident through the QCERT Portal.



Responding to an QCERT Incident through the QCERT Portal

REPORT → REGISTER → MANAGE → UPDATE → RECOVERY