GARIS PANDUAN
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

MAJLIS DAERAH PEKAN

11 OKTOBER 2022

ISI KANDUNGAN

TUJUAN

Garis Panduan ini menjelaskan mengenai Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) dan peranan *Computer Emergency Response Team* (CERT) MDP-MDP di bawah MDP di dalam mengurus pengendalian insiden keselamatan ICT selaras dengan pematuhan terhadap peraturan yang telah ditetapkan dalam Dasar Keselamatan ICT MDP Versi 2.0 iaitu Perkara 9 Pengurusan Pengendalian Insiden Keselamatan dan Perkara 2 Organisasi Keselamatan.

PENGENALAN

Garis Panduan ini disediakan bagi memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan ICT termasuk mengenal pasti ancaman dan kelemahan di semua MDP.

MDP telah menggunakan mekanisme prosedur pelaporan insiden keselamatan ICT berdasarkan pekeliling-pekeliling seperti berikut:

a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi;

b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan

c) Surat Ketua Pengarah Keselamatan Negara, Majlis Keselamatan Negara – Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team* (GCERT) Oleh MDP Keselamatan Siber Negara (NACSA) yang bertarikh 28 Januari 2019.

SKOP

Skop dokumen ini digunapakai dalam "*ISO 27001: 2013 Information Security Management System (ISMS)*".

TAKRIFAN

a) **MDP MDP** – MDP di bawah pentadbiran MDP terdiri daripada Pejabat Yang Dipertua, Jabatan Khidmat Pengurusan, Jabatan Perbendaharaan, Jabatan Penilaian, Jabatan Perancang Bandar, Jabatan Kejuruteraan, Jabatan Perkhidmatan Perbandaran, Jabatan Penguatkuasaan & Keselamatan, Jabatan Perhubungan Awam & Komuniti, Bahagian Landskap & Rekreasi, Bahagian Kawalan Bangunan, Bahagian Pusat Setempat, Bahagian Teknologi Maklumat, Bahagian Integriti & Audit Dalam, Bahagian Undang-Undang dan Bahagian Ukur Bahan.

b) **ICTSO** – *ICT Security Officer*. Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.

c) **NACSA** – MDP Keselamatan Siber Negara (*National Cyber Security Agency* (NACSA)). MDP pusat yang bertanggungjawab ke atas semua aspek keselamatan siber bagi memantapkan pengurusan keselamatan siber negara.

d) **Perkakasan ICT** – Merangkumi semua jenis perkakasan atau peranti elektronik yang diperlukan untuk melaksanakan sesuatu projek ICT iaitu peralatan input/output (contoh: pencetak, pengimbas, alat baca biometrik, Suara Melalui IP (VoIP), pemprosesan, storan data, multimedia [contoh: persidangan video (video conferencing)], perkakasan komunikasi mudah alih [contoh: jalur lebar tanpa wayar (*wireless broadband*)] dan perkakasan Komunikasi berteknologi tinggi (contoh: radar, satelit).

1. INSIDEN KESELAMATAN ICT

1.1 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 sama ada yang ditetapkan secara tersurat atau tersirat.

1.2 Insiden Keselamatan ICT terbahagi kepada dua (2) iaitu Insiden Keselamatan Siber dan Insiden Keselamatan Bukan Siber.

1.3 Insiden keselamatan siber yang dikenalpasti adalah seperti berikut:-

(a) Penafian Perkhidmatan (*Denial-of-Service / Distributed Denial-of-Service (DDoS)*)
Ancaman ke atas ketersediaan operasi dan sistem komputer. Ia melibatkan sebarang tindkan yang menghalang sistem daripada berfungsi secara normal.

(b) Pencerobohan (*Intrusion*)
Akses yang tidak dibenarkan dan tidak sah ke atas sistem atau rangkaian dan berupaya mengubah kandungan sistem/rangkaian tersebut.

(c) Cubaan Pencerobohan (*Intrusion Attempt*)
Percubaan untuk akses yang tidak dibenarkan dan tidak sah ke atas sistem atau rangkaian.

(d) Jangkitan Perisian Merbahaya (*Malware Infection*)
Perisian atau skrip komputer yang diprogramkan untuk menceroboh komputer dan merosakkan sistem.

(e) Penghosan Perisian Merbahaya (*Malware Hosting*)
Pelayan atau komputer yang telah dijangkiti oleh perisian berbahaya dan bertindak sebagai pusat penyebaran perisian berbahaya kepada pelawat sistem/laman sesawang.

(f) Potensi Serangan (*Potential Attack*)
Kemungkinan berlaku serangan menggunakan kelemahan yang terdapat pada sistem atau rangkaian.

(g) 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*).

(h) 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.

(i) Harrassment/Threats

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

14 Manakala insiden keselamatan yang dikategorikan sebagai insiden keselamatan bukan siber adalah 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) Kehilangan Fizikal (*Physical Loss*)

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

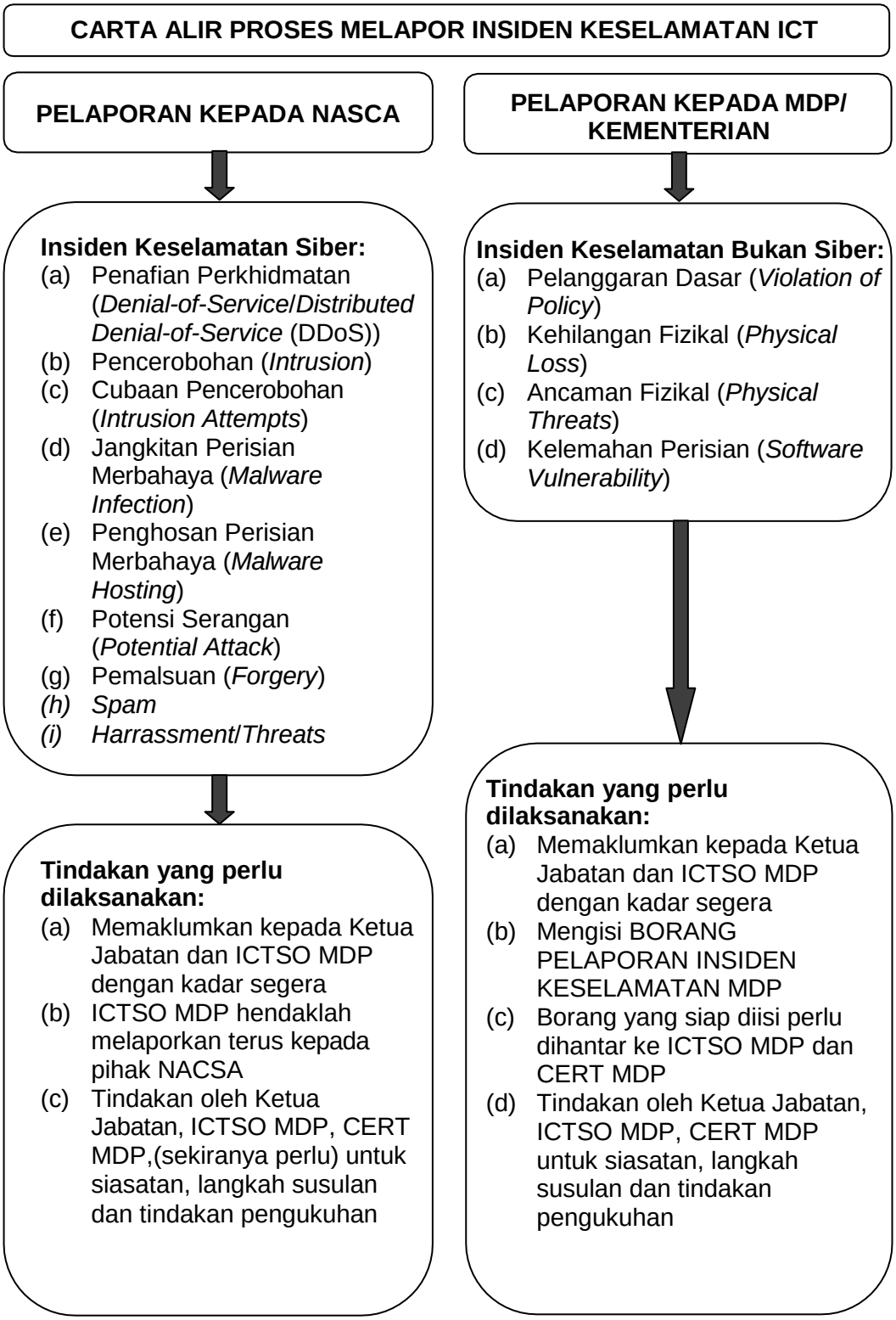
(c) Ancaman Fizikal (*Physical Threats*)

Ancaman yang menyebabkan kerosakan kepada perkakasan dan infrastruktur sistem komputer. Ini termasuk perkakasan ICT yang rosak, usang dan tidak boleh dibaiki seperti CPU, *hard disk* dan sebagainya.

(d) Kelemahan Perisian (*Software Vulnerability*)

Kelemahan perisian adalah lubang keselamatan (*security hole*) atau kelemahan yang terdapat dalam perisian sistem, perisian aplikasi, sistem operasi dan lesen perisian. Kelemahan perisian ini disebabkan oleh perisian tidak dikemaskini, perisian tiada penampalan dan perisian tidak berlesen.

15 Gangguan atau ancaman yang menyebabkan kegagalan dalam penyampaian perkhidmatan bagi para di atas diringkaskan seperti berikut:



2. TAHAP KEUTAMAAN TINDAKAN KE ATAS INSIDEN

2.1 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.

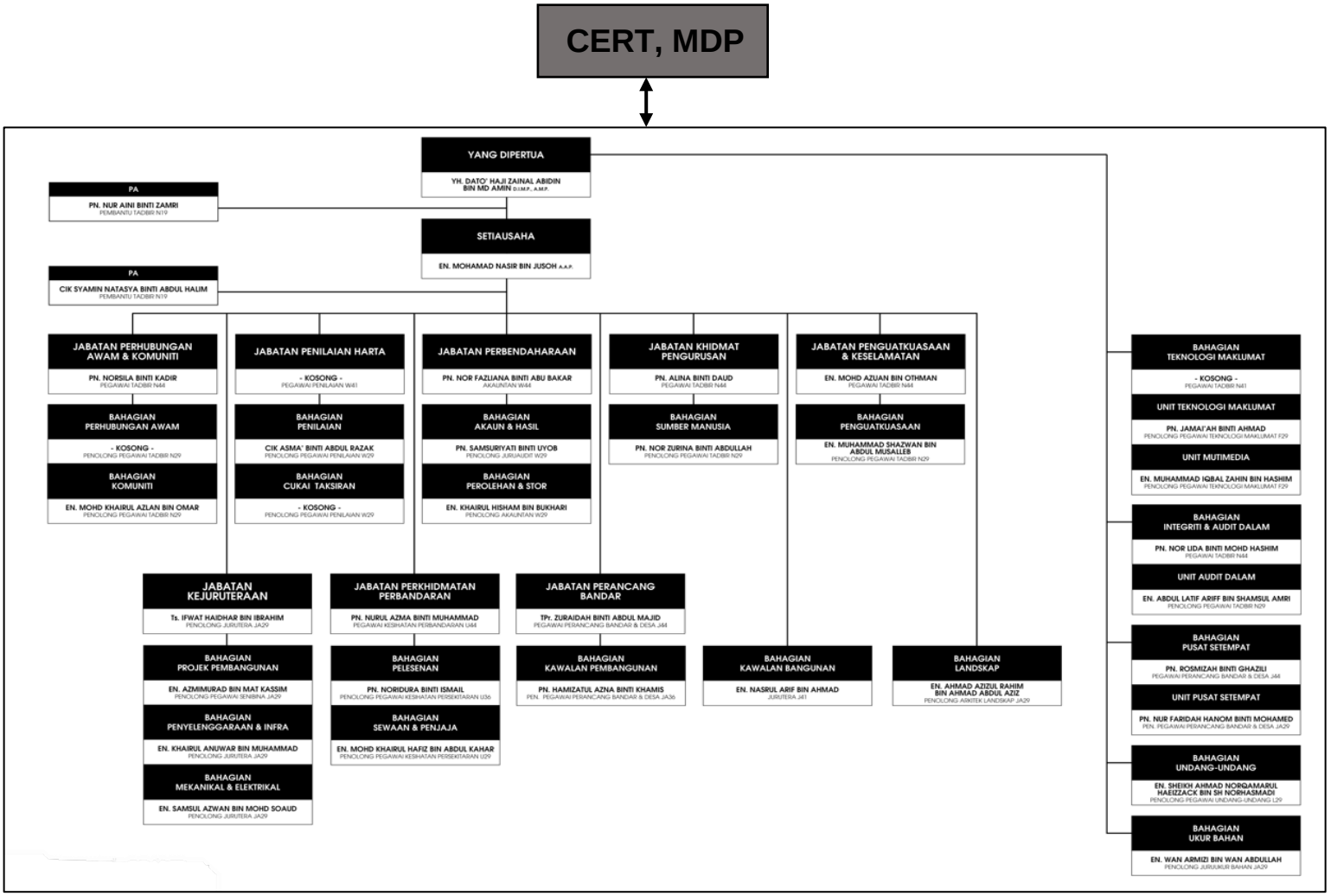
(b) Keutamaan 2 (Kuning) – insiden keselamatan ICT selainnya seperti pencerobohan laman web, gangguan sistem dan pencerobohan aset ICT.

3. PENUBUHAN CERT MDP

3.1 Bagi memperkukuhkan pengurusan pengendalian insiden ICT, Pejabat Cawangan seperti Pejabat Kelab Golf Diraja Pekan, Pejabat Taman Tasik Sultan Abu Bakar, dan Pejabat Chini hendaklah menubuhkan CERT Cawangan masing-masing. CERT Cawangan bertindak sebagai *first level support* kepada CERT MDP dalam mengendali insiden keselamatan ICT, mengawasi dan memberi khidmat nasihat berkaitan keselamatan ICT.

3.2 MDP akan menggunakan struktur model CERT MDP seperti berikut:-

PASUKAN CERT MDP



3.3 Keahlian CERT MDP yang dicadangkan adalah seperti berikut :

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

3.4 Keahlian CERT MDP boleh dilantik dari kalangan anggota sedia ada yang mengendalikan operasi komputer.

3.5 MDP hendaklah menggunakan Borang Pelantikan CERT MDP seperti di **Lampiran 1**. Manakala bagi pengemaskinian maklumat CERT MDP hendaklah menggunakan Borang Kemaskini CERT MDP seperti di **Lampiran 2**.

4. TANGGUNGJAWAB KETUA JABATAN

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

5. TANGGUNGJAWAB CERT MDP

5.1 Tanggungjawab CERT MDP meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan ICT yang dialami oleh MDP 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 CERT MDP sama ada sebagai input atau untuk tindakan seterusnya;

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

(f) Menyebarkan makluman berkaitan insiden kepada MDP 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.

5.2 Apabila berlaku insiden, Pengarah CERT MDP perlu menggerakkan ahli CERT MDP untuk mengambil tindakan berikut :-

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

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

(c) Menentukan sama ada insiden ini perlu dilaporkan kepada MDP penguatkuasaan undang-undang/keselamatan.

6. PROSES PELAPORAN INSIDEN KESELAMATAN ICT

6.1 Setiap insiden keselamatan siber yang berlaku hendaklah dilaporkan kepada pihak NACSA. Proses Kerja Pelaporan Insiden Keselamatan Siber seperti di **Lampiran 3**. Manakala bagi insiden keselamatan bukan siber, pelapor perlu mengisi Borang Laporan Insiden Keselamatan MDP seperti di **Lampiran 4.** Borang ini hendaklah diemelkan kepada CERT MDP.

6.2 Bagi memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan, mekanisma pelaporan Insiden Keselamatan ICT adalah seperti berikut:

(a) Semua pelapor perlu segera melaporkan sebarang kejadian insiden keselamatan ICT bagi mengelakkan kerosakan bahan bukti tanpa melaksanakan tindakan secara sendirian.

(b) Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO MDP dan CERT MDP. Semua maklumat adalah SULIT dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan sahaja.

(c) CERT MDP akan bertindak dan menghubungi NACSA sebagai makluman atau bagi mendapatkan bantuan sekiranya perlu.

7. PENUTUP

7.1 Garis panduan ini disediakan untuk membantu *Computer Emergency Response Team* (CERT) MDP memperkemaskan pengurusan pengendalian insiden keselamatan ICT dan memperkasakan MDP menguruskan sendiri pengendalian insiden keselamatan ICT di MDP masing-masing.

LAMPIRAN 1 : BORANG PELANTIKAN CERT AGENSI

Borang CERT-01

BORANG PERLANTIKAN
COMPUTER EMERGENCY RESPONSE TEAM (CERT) AGENSI

MAKLUMAT CERT AGENSI

Nama CERT Agensi :_____
Kementerian / Kerajaan Negeri :_____
Jabatan / Badan Berkanun / Agensi : _____
Alamat : _____
_____
No. Tel. :_____No. Faks : _____
Tarikh Penubuhan :_____Ruj. Kelulusan : _____
E-mel CERT Agensi : _____

MAKLUMAT PENGARAH CERT

Nama :_____
No. Kad Pengenalan: _____
Jawatan :_____Gred : _____
*Peranan : CIO / CISO / ICTSO / Lain-lain (Sila nyatakan :_____)
No. Tel. Pejabat :_____No. Tel. Bimbit :_____
E-mel : _____

MAKLUMAT PENGURUS CERT

Nama :_____
No. Kad Pengenalan: _____
Jawatan :_____Gred : _____
*Peranan : ICTSO / Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :_____)
No. Tel. Pejabat :_____No. Tel. Bimbit :_____
E-mel :_____

MAKLUMAT AHLI CERT

Nama : _____
No. Kad Pengenalan: _____
Jawatan : _____Gred : _____

*Peranan : Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :____________________)

No. Tel. Pejabat : ____________________No. Tel. Bimbit :________________________
E-mel : ____
**Nama Agensi : ____

Nama :____
No. Kad Pengenalan: ____
Jawatan :______________________________________Gred : ________________
*Peranan : Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :____________________)
No. Tel. Pejabat : ____________________No. Tel. Bimbit :________________________
E-mel : ____
**Nama Agensi : ____

Nama :____
No. Kad Pengenalan: ____
Jawatan :______________________________________Gred : ________________
*Peranan : Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :____________________)
No. Tel. Pejabat : ____________________No. Tel. Bimbit :________________________
E-mel : ____
**Nama Agensi : ____

Nama :____
No. Kad Pengenalan: ____
Jawatan :______________________________________Gred : ________________
*Peranan : Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :____________________)
No. Tel. Pejabat : ____________________No. Tel. Bimbit :________________________
E-mel : ____
**Nama Agensi : ____

Nama :____
No. Kad Pengenalan: ____
Jawatan :______________________________________Gred : ________________
*Peranan : Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :____________________)
No. Tel. Pejabat : ____________________No. Tel. Bimbit :________________________
E-mel : ____
**Nama Agensi : ____

PENGESAHAN KETUA JABATAN/ KETUA PEGAWAI MAKLUMAT (CIO)

Nama :_____

Jawatan :_____

No. Tel. Pejabat:_____No. Faks : _____

Tandatangan :_____Tarikh : _____

Borang pelantikan *Computer Emergency Response Team* (CERT) Agensi yang telah lengkap hendaklah dikemukakan ke alamat seperti berikut :-

Ketua Pengarah Keselamatan Negara
Majlis Keselamatan Negara
Aras LG & G, Blok Barat
Bangunan Perdana Putra
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA
(u/p.: National Cyber Corrdination and Command Centre (NC4))

Atau melalui:
Faksimili – 03-8064 4846 (u/p.: National Cyber Corrdination and Command Centre (NC4))
E-mel – ictso@nacsa.gov.my (borang lengkap dan diimbas)

NOTA :

*** Peranan – Pilih yang berkaitan**

**** Tuliskan nama agensi sekiranya berlainan dengan yang dinyatakan dalam ruangan Maklumat CERT Agensi**

LAMPIRAN 2 : BORANG KEMASKINI CERT AGENSI

Borang CERT-02

BORANG KEMASKINI MAKLUMAT AHLI
COMPUTER EMERGENCY RESPONSE TEAM (CERT) AGENSI

MAKLUMAT CERT AGENSI

Nama CERT Agensi :_____
Kementerian / Kerajaan Negeri :_____
Jabatan / Badan Berkanun / Agensi : _____
E-mel kumpulan (group e-mel) : _____

MAKLUMAT PENAMBAHAN AHLI BAHARU CERT

Nama :_____
No. Kad Pengenalan: _____
Jawatan/Gred : _____
*Peranan : CIO / CISO / ICTSO / Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :_____)
Keahlian : ☐ Pengarah CERT ☐ Pengurus CERT ☐ Ahli CERT
No. Tel. Pejabat :_____No. Tel. Bimbit :_____
E-mel :_____
Tarikh menyertai CERT : _____
**Agensi : _____

Nama :_____
No. Kad Pengenalan: _____
Jawatan/Gred : _____
*Peranan : CIO / CISO / ICTSO / Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :_____)
Keahlian : ☐ Pengarah CERT ☐ Pengurus CERT ☐ Ahli CERT
No. Tel. Pejabat :_____No. Tel. Bimbit :_____
E-mel :_____
Tarikh menyertai CERT : _____
** Agensi : _____

Nama : _____

No. Kad Pengenalan: _____

Jawatan/Gred : _____

*Peranan : CIO / CISO / ICTSO / Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :_____)

Keahlian : ☐ Pengarah CERT ☐ Pengurus CERT ☐ Ahli CERT

No. Tel. Pejabat :_____ No. Tel. Bimbit :_____

E-mel :_____

Tarikh menyertai CERT : _____

** Agensi : _____

Nama : _____

No. Kad Pengenalan: _____

Jawatan/Gred : _____

*Peranan : CIO / CISO / ICTSO / Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :_____)

Keahlian : ☐ Pengarah CERT ☐ Pengurus CERT ☐ Ahli CERT

No. Tel. Pejabat :_____ No. Tel. Bimbit :_____

E-mel :_____

Tarikh menyertai CERT : _____

** Agensi : _____

MAKLUMAT AHLI YANG BERTUKAR

Nama : _____

No. Kad Pengenalan: _____

Jawatan/Gred : _____

*Peranan : CIO / CISO / ICTSO / Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :_____)

Keahlian : ☐ Pengarah CERT ☐ Pengurus CERT ☐ Ahli CERT

No. Tel. Pejabat :_____ No. Tel. Bimbit :_____

E-mel :_____

Tarikh bertukar : _____

Tempat ditukarkan: _____

Nama :_____

No. Kad Pengenalan: _____

Jawatan/Gred : _____

*Peranan : CIO / CISO / ICTSO / Pentadbir Sistem / Pentadbir Rangkaian / Pentadbir Server / Pentadbir Laman Web / Lain-lain (Sila nyatakan :_____)

Keahlian : ☐ Pengarah CERT ☐ Pengurus CERT ☐ Ahli CERT

No. Tel. Pejabat :_____ No. Tel. Bimbit :_____

E-mel :_____

Tarikh bertukar : _____

Tempat ditukarkan: _____

PENGESAHAN KETUA JABATAN/ KETUA PEGAWAI MAKLUMAT (CIO)

Nama :_____

Jawatan/ Gred : _____

No. Tel. Pejabat:_____ No. Faks : _____

E-mel : _____

Tandatangan :_____ Tarikh : _____

Borang pelantikan *Computer Emergency Response Team* (CERT) Agensi yang telah lengkap hendaklah dikemukakan ke alamat seperti berikut :-

Ketua Pengarah Keselamatan Negara
Majlis Keselamatan Negara
Aras LG & G, Blok Barat
Bangunan Perdana Putra
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA
(u/p.: National Cyber Corrdination and Command Centre (NC4))

Atau melalui:
Faksimili – 03-8064 4846 (u/p.: National Cyber Corrdination and Command Centre (NC4))
E-mel – ictso@nacsa.gov.my (borang lengkap dan diimbas)

NOTA :

*** Peranan – Pilih yang berkaitan**

**** Tuliskan nama agensi sekiranya berlainan dengan yang dinyatakan dalam ruangan Maklumat CERT Agensi**

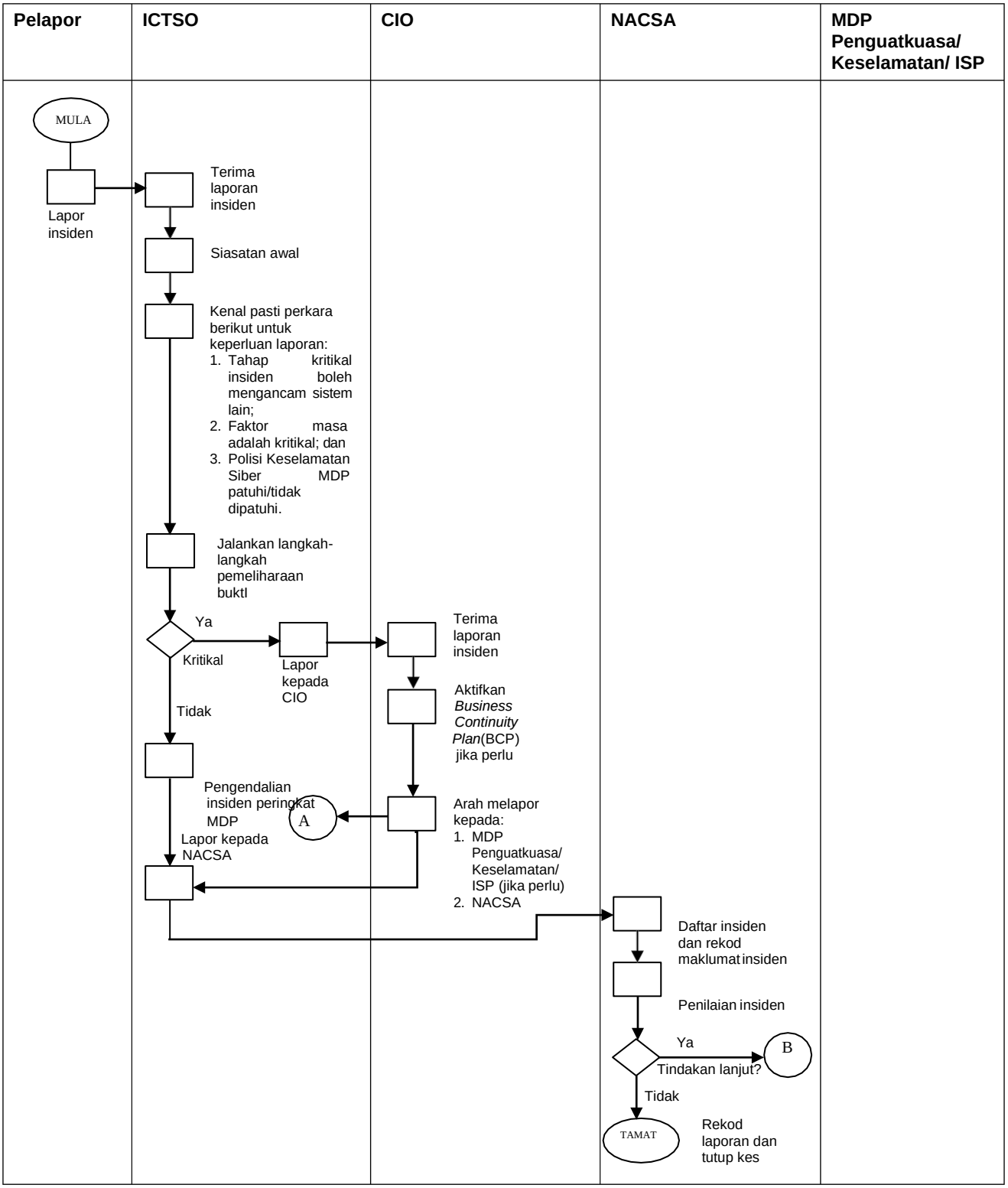
LAMPIRAN 3 : PROSEDUR PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

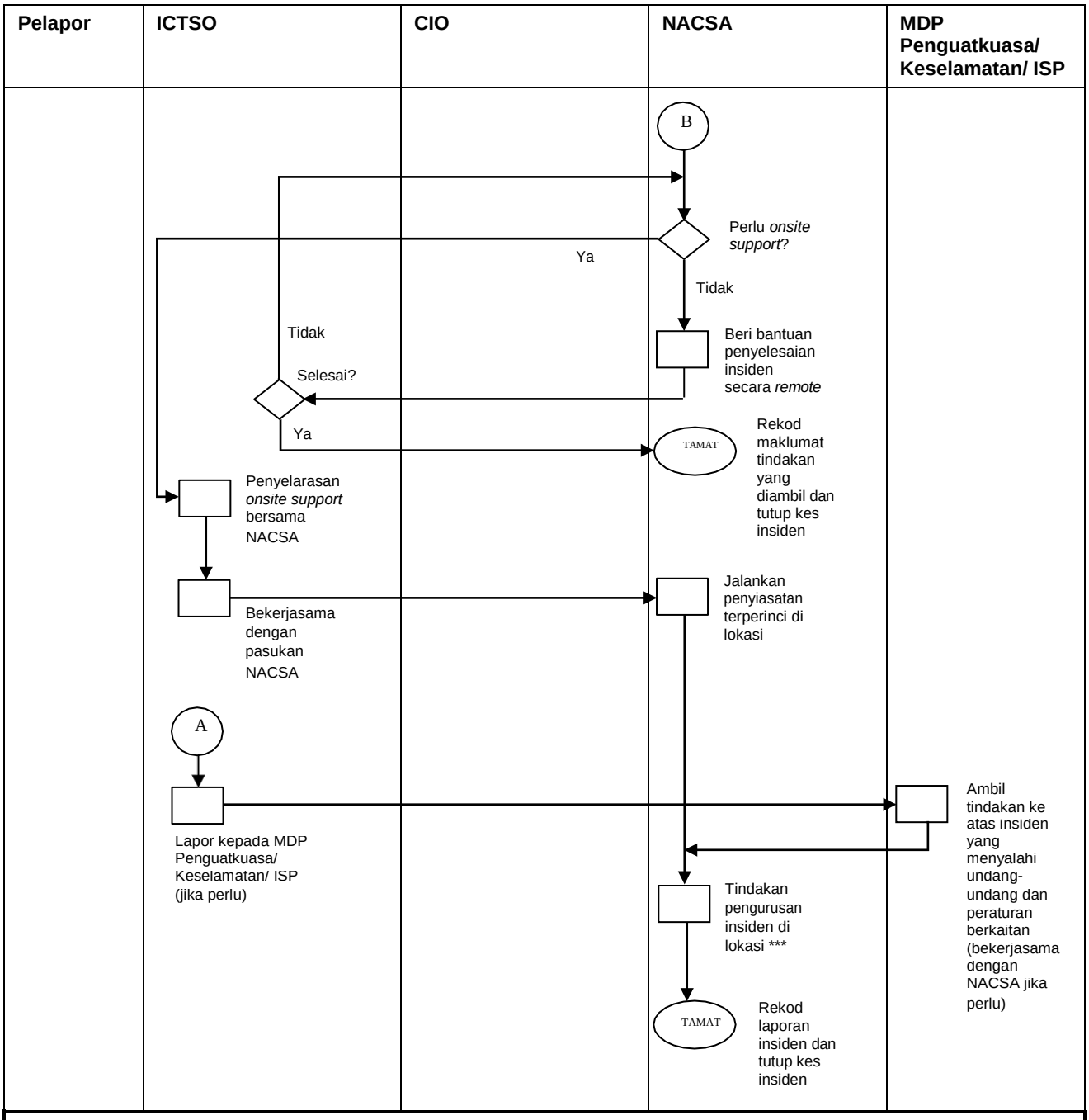
Pengurusan Insiden Keselamatan Maklumat				
Proses Kerja	**Prosedur**	**Borang/ Dokumen**	**Tanggunjawab**	
			Pelaksana	**Kelulusan**
1.0 Melaporkan insiden keselamatan maklumat	1.0 Adalah tanggungjawab semua pihak untuk melaporkan sebarang insiden keselamatan maklumat yang berlaku di organisasi kepada jabatan ICT. Jabatan IT telah mewujudkan garis panduan kriteria insiden keselamatan maklumat dan kategori (Rujuk Att. A)	Email / Sistem	PPTM/ JTK / warga kerja / Pembekal	Ketua Jabatan ICT
2.0 Kerahan 1st level support	2.0 Ketua Jabatan IT akan mengarahkan "1st level support" untuk mengenalpasti menyelesaikan insiden keselamatan maklumat.	-	PPTM/ JTK / Pembekal	Ketua Jabatan ICT
3.0 Insiden Keselamatan Maklumat "*Escalation*"	3.0 Jika insiden tersebut tidak dapat diselesaikan, lokasi insiden perlu dikawal dengan keadah yang sepatutnya – Bergantung kepada jenis insiden. Jabatan IT mungkin memerlukan khidmat pembekal untuk menyelesaikan insiden tersebut.	- -	PPTM/ JTK / Pembekal	Ketua Jabatan ICT
4.0 Analisa Insiden Keselamatan Maklumat	4.0 Jabatan IT / pembekal perlu mengenalpasti analogi insiden, analisis punca utama dan hasil siasatan insiden.	Laporan Insiden Keselamatan Maklumat	PPTM/ JTK / Pembekal	Ketua Jabatan ICT
5.0 Laporan	5.0 Jabatan IT / Pembekal perlu menyediakan laporan lengkap insiden keselamatan maklumat dan maklumkan kepada pengurusan tertinggi organisasi	Laporan Insiden Keselamatan Maklumat	PPTM/ JTK / Pembekal	Yang Dipertua

LAMPIRAN 4 : KRITERIA INSIDEN KESELAMATAN MAKLUMAT

Klasifikasi Insiden	**Description**	**Dilaporkan dalam Tempoh (Oleh Pelapor)**	**Sasaran Penyelesaian (*Resolution Target*)**
High (*Tinggi*)	Berpotensi untuk berlaku bencana merangkumi keseluruhan servis utama organisasi serta melibatkan maklumat kritikal pelanggan atau merencatkan proses kerja utama organisasi melebihi tempoh 4 jam. *Potential to become a disaster covering entire services organization, involving critical customer data or extended disruption or disturbance for more than 4 hours*	1 Jam	3 Hari
Medium (*Sederhana*)	Berpotensi untuk berlakunya kecemasan diperingkat operasi syarikat atau di sesebuah jabatan dalam organisasi atau menjejaskan proses kerja/perkhidmatan kepada pelanggan untuk tempoh 1-4 jam. *Potential to become an emergency effecting only local site or disturbance/disruption to customers (internal or external) between 1-4 hours*	24 Jam	30 Hari
Low (*Rendah*)	Bukan dikategorikan sebagai insiden bencana IT atau berlaku “glitch” namun tidak menjejaskan proses perkhidmatan pada sistem utama syarikat. Insiden boleh diselesaikan dalam tempoh 1 jam setelah laporan diterima. *Not a serious event, effect minimal (SLA not breached) on critical business processes and can be rectified within 1 hour*	72 Jam	90 Hari

LAMPIRAN 5 : CARTA ALIRAN PROSES KERJA PELAPORAN INSIDEN KESELAMATAN SIBER





***** Tindakan pengurusan insiden di lokasi:**

1. Kawal kerosakan;
2. Baik pulih minima dengan segera;
3. Siasat insiden dengan terperinci;
4. Analisis impak (*Business Impact Analysis*);
5. Hasilkan laporan insiden;
6. Bentang dan kemukakan laporan kepada MDP; dan
7. Selaraskan tindakan di antara MDP d an MDP Penguatkuasa/Keselamatan/ISP (jika berkenaan).

LAMPIRAN 6 : BORANG PELAPORAN INSIDEN KESELAMATAN MDP

LAPORAN INSIDEN BAGI MDP _____

A. MAKLUMAT INSIDEN			
1.	**Jenis Insiden**	**:**	
2.	**Keutamaan (*Severity*) Insiden**	**:**	☐ **High** (Indicator of compromise is found on reported CNII Assets)
			☐ **Medium** (Found indicators showing reported CNII Assets is under malicious attack)
			☐ **Low** (Found suspicious attempt on reported CNII Assets directly or indirectly)
3.	**Tarikh & Masa Insiden Bermula**	**:**	
4.	**Tarikh & Masa Insiden Tamat**	**:**	
5.	**Serangan Yang Dikesan**	**:**	
6.	**Keterangan Ringkas Insiden (URL/Nama system)**	**:**	
7.	**Aset Fizikal Yang Terkesan (Domain & Nama Aset)**	**:**	
8.	**Jumlah Host Yang Terkesan**	**:**	
9.	**Ancaman Yang Dijumpai (Jika Ada Berikan Jenis, Kesan, Tindakan Pulih)**	**:**	
10.	***Onsite Request* (Jika Ada Minta Bantuan Luar)**	**:**	
11.	**Serangan Terdahulu (Jika Ada Berikan Tajuk Insiden, Status, Tarikh Terakhir Baik Pulih)**	**:**	
12.	**Pembangunan Sistem (*Outsource* atau Dalaman)**	**:**	
B. MAKLUMAT ASET FIZIKAL			
1.	**Nama MDP**	**:**	
2.	**CPE (*Hardware* (*Brand*/ *Model*/ *Version*))**	**:**	
3.	**GUID (*MAC Address Server*)**	**:**	
4.	**Spesifikasi Komputer**	**:**	
5.	**Maklumat Perisian (Jenis/ Version)**	**:**	
6.	**Maklumat Rangkaian (*IP Address*)**	**:**	
7.	**Maklumat Pangkalan Data (Jenis/ *Version*)**	**:**	
8.	**Maklumat Service (*Host*/ *Port*/ *Protocol*)**	**:**	
9.	**Maklumat *Circuit* (*Device Name*)**	**:**	
10.	**Maklumat Website/Portal (*Document Root*/ *Locale*)**	**:**	

C. KRONOLOGI KEJADIAN		
TARIKH	**MASA**	**KETERANGAN**

D. RINGKASAN INSIDEN

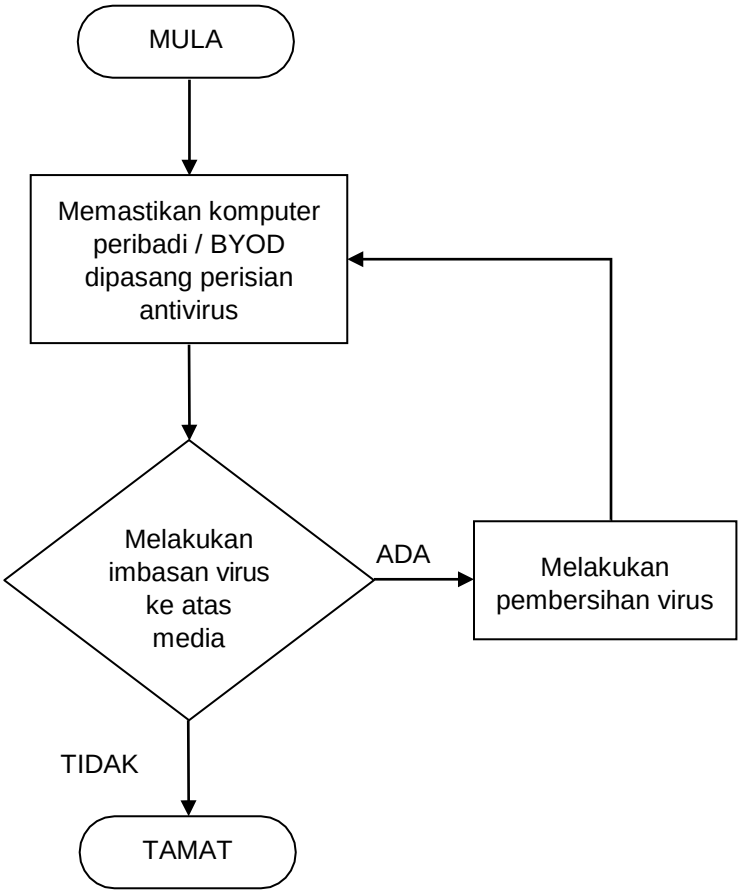
1. **Keterangan mengenai insiden termasuk impak MDP dan pengguna.**
2. **Senarai langkah-langkah pengukuhan yang telah diambil.**
3. **Nyatakan jangkaan tindakan selesai.**

LAMPIRAN 7 : PROSEDUR KESELAMATAN DARI ANCAMAN VIRUS

5.1 Proses Kerja

Bil	Proses Kerja
1.	Memastikan komputer yang digunakan dipasang dengan perisian antivirus yang terkini dan mempunyai keupayaan untuk mengesan jangkitan virus.
2.	Memastikan Komputer Riba (*Bring Your Own Device* (BYOD)) dilengkapi dengan perisian antivirus terkini termasuk komputer riba yang dibawa oleh pihak kontraktor/ketiga.
3.	Pengguna hendaklah sentiasa melakukan imbasan virus (*virus scanning*) terhadap semua media yang dibawa dari luar seperti *thumb drive* dan *external hard disk* untuk mengawal keselamatan maklumat dan data dari dirosakkan oleh serangan virus.
4.	Sekiranya media tersebut dikesan dijangkiti oleh virus, ianya hendaklah dibuat pembersihan sebelum digunakan.
5.	Pengguna adalah dikehendaki melakukan imbasan virus sekerap yang mungkin atau secara berkala bagi memastikan ia bebas dari virus.
6.	Mengemaskini perisian antivirus secara berkala.

5.2 CARTA ALIR PROSEDUR KESELAMATAN DARI ANCAMAN VIRUS



LAMPIRAN 8 : RUJUKAN

1. Dasar Keselamatan ICT Majlis Daerah Pekan 2.0
2. *ISO 27001: 2013 Information Security Management System (ISMS)*
3. Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
4. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)
5. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
6. Surat Ketua Pengarah Keselamatan Negara, Majlis Keselamatan Negara – Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team* (GCERT) Oleh MDP Keselamatan Siber Negara (NACSA) yang bertarikh 28 Januari 2019