



**KERAJAAN MALAYSIA**

---

**PEKELILING AM BILANGAN 4 TAHUN 2022**

---

**PENGURUSAN DAN PENGENDALIAN INSIDEN KESELAMATAN  
SIBER SEKTOR AWAM**

**JABATAN PERDANA MENTERI**

**1 Ogos 2022**

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian

Semua Ketua Jabatan Persekutuan

Semua YB Setiausaha Kerajaan Negeri

Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri

Semua Pihak Berkuasa Tempatan



**JABATAN PERDANA MENTERI  
PRIME MINISTER'S DEPARTMENT**

Blok B8, Kompleks Jabatan Perdana Menteri  
Pusat Pentadbiran Kerajaan Persekutuan  
62502 Putrajaya  
MALAYSIA

Tel. : 03-8000 8000  
Fax : 03-8888 3904  
Web : <http://www.jpm.gov.my>  
Emel : [jpm@jpm.gov.my](mailto:jpm@jpm.gov.my)

---

Rujukan Kami: MKN.10.700-8/151 JLD 2 ( 9 )

Tarikh: | Ogos 2022

Semua Ketua Setiausaha Kementerian

Semua Ketua Jabatan Persekutuan

Semua YB Setiausaha Kerajaan Negeri

Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri

Semua Pihak Berkuasa Tempatan

---

**PEKELILING AM BILANGAN 4 TAHUN 2022**

---

**PENGURUSAN DAN PENGENDALIAN INSIDEN KESELAMATAN  
SIBER SEKTOR AWAM**

**1. TUJUAN**

- 1.1 Pekeliling Am ini bertujuan menjelaskan tatacara pengurusan dan pengendalian insiden keselamatan siber bagi sektor awam seperti yang berikut:

- (i) Mengenal pasti tahap keutamaan tindakan terhadap insiden keselamatan siber supaya satu pendekatan yang seragam dan proaktif dapat dilaksanakan secara berkesan.
- (ii) Menetapkan penubuhan, fungsi, tanggungjawab, dan struktur Pasukan Tindak Balas Insiden Keselamatan Siber [(*Cyber Security Incident Response Team*, (CSIRT))] agensi.
- (iii) Menggariskan bidang tugas dan tanggungjawab Ketua Jabatan, CSIRT Agensi dan Pusat Penyelarasan dan Kawalan Siber Negara [*National Cyber Coordination and Command Centre*, (NC4)] dalam pengurusan dan pengendalian insiden keselamatan siber bagi sektor awam.
- (iv) Menerangkan proses kerja pelaporan insiden dan Prosedur Operasi Standard [(*Standard Operating Procedure*, (SOP))] pengendalian insiden.

## 2. TAFSIRAN

2.1 Bagi tujuan Pekeliling Am ini yang hanya terpakai kepada sektor awam, terma di bawah ditafsirkan seperti yang berikut:

- (i) “**Agensi**” ialah agensi sektor awam yang merangkumi kementerian dan jabatan pada peringkat pentadbiran Kerajaan, Kerajaan Persekutuan, Badan Berkanun

Persekutuan, Pejabat Setiausaha Kerajaan (SUK) Negeri, Badan Berkanun Negeri serta Pihak Berkuasa Tempatan (PBT).

- (ii) **“Ancaman siber”** ialah ancaman yang berpunca daripada Internet atau rangkaian menggunakan laluan komunikasi data yang memberi kesan terhadap kerahsiaan, integriti dan ketersediaan sistem maklumat dari dalam sesebuah organisasi mahupun dari jarak jauh, serta penyebaran maklumat melalui medium siber yang bertentangan dengan undang-undang negara dan berupaya menggugat keselamatan negara.
  
- (iii) **“CSIRT Agensi”** ialah pasukan tindak balas insiden keselamatan siber yang merangkumi kementerian dan jabatan pada peringkat pentadbiran Kerajaan, Kerajaan Persekutuan, Badan Berkanun Persekutuan, Pejabat Setiausaha Kerajaan (SUK) Negeri, Badan Berkanun Negeri serta Pihak Berkuasa Tempatan (PBT).
  
- (iv) **“Infrastruktur Maklumat Kritikal Negara” (Critical National Information Infrastructure, CNII)** merujuk kepada sistem kritikal yang merangkumi aset maklumat (elektronik), rangkaian, fungsi, proses, kemudahan, dan perkhidmatan dalam persekitaran teknologi maklumat dan komunikasi (Information and Communications Technology, ICT) yang penting kepada negara di mana sebarang gangguan atau

kemusnahan ke atasnya boleh memberi impak kepada pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan Kerajaan untuk berfungsi, kesihatan, dan keselamatan awam serta privasi individu.

- (v) **“Insiden keselamatan siber”** ialah kejadian siber yang tidak diingini apabila berlakunya kehilangan kerahsiaan maklumat, gangguan terhadap integriti data atau sistem, atau gangguan yang menyebabkan kegagalan dalam memperoleh maklumat daripada sistem komputer dan kemungkinan berlakunya kesalahan pelanggaran peraturan keselamatan maklumat, dasar-dasar tertentu atau amalan piawai keselamatan siber.
- (vi) **“Krisis Siber Negara”** ialah suatu keadaan di mana insiden keselamatan siber melebihi tahap yang ditetapkan sehingga menjejaskan kerahsiaan, integriti, dan ketersediaan agensi sektor awam terutamanya agensi CNII dan memberi impak terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan Kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu.
- (vii) **“Prosedur Tindak Balas, Komunikasi dan Penyelarasan Pengurusan Krisis Siber Negara”** ialah proses pengurusan insiden dan langkah-langkah

yang perlu diambil oleh pihak yang berkaitan dalam Pengurusan Krisis Siber Negara.

- (viii) **“Pengurusan Krisis Siber Negara”** ialah satu pendekatan sistematik bagi pencegahan, persediaan, tindak balas, dan pemulihan daripada insiden keselamatan siber terhadap CNII.

### 3. LATAR BELAKANG

3.1 Mesyuarat Jemaah Menteri pada 20 Januari 2016, 13 Julai 2016 dan 11 Januari 2017 telah bersetuju pewujudan Agensi Keselamatan Siber Negara (National Cyber Security Agency, NACSA) yang diletakkan di bawah Majlis Keselamatan Negara, Jabatan Perdana Menteri (MKN, JPM). Penubuhan NACSA sebagai satu agensi pusat khusus yang bertanggungjawab atas semua aspek keselamatan siber menunjukkan komitmen Kerajaan Malaysia dalam menangani ancaman siber. Susulan daripada keputusan tersebut, penubuhan NACSA telah berkuat kuasa pada 1 Februari 2017.

3.2 NACSA berperanan sebagai satu agensi yang bertanggungjawab kepada usaha mempertingkatkan tahap kesiapsiagaan keselamatan siber negara dengan memperkukuh tindakan menangani ancaman siber yang merangkumi:

- (i) Pembangunan dan pelaksanaan dasar serta strategi pengurusan keselamatan siber negara.
- (ii) Pelaksanaan tindakan strategik bagi menangani ancaman siber.
- (iii) Perlindungan terhadap sistem kritikal negara.
- (iv) Pembudayaan dan pembangunan keupayaan.

3.3 Selain itu, NACSA bertanggungjawab dalam pelaksanaan perancangan strategik, tindakan bersepadu atas jenayah siber, pengurusan risiko keselamatan siber, pengurusan sumber optimum melalui pemusatan kepakaran, pembangunan sistem aplikasi berkaitan keselamatan siber yang bersepadu yang merentas pelbagai agensi pada peringkat nasional dan antarabangsa.

3.4 NACSA juga telah menubuhkan NC4 sebagai sebuah pusat operasi siber bagi memantapkan penyelarasan dan kawalan bersepadu keselamatan siber negara. NC4 berperanan sebagai tempat rujukan dan perhubungan utama berkaitan keselamatan siber negara oleh semua organisasi dalam dan luar negara serta bertanggungjawab dalam mengurus dan memantau ancaman siber terhadap sistem-sistem kritikal negara, memastikan kesiapsiagaan, pelaksanaan tindak balas serta mitigasi insiden keselamatan siber pada peringkat strategik dan taktikal.

- 3.5 Selaras dengan peranan tersebut, Sidang Majlis Keselamatan Negara Bilangan 3/2021 pada 13 Julai 2021 telah memutuskan NC4 sebagai Pasukan Tindak Balas Kecemasan Komputer Negara [*National Computer Emergency Response Team, National (CERT)*] dan perkara ini turut dinyatakan dalam Arahan Majlis Keselamatan Negara No. 26: Pengurusan Keselamatan Siber Negara tahun 2021.
- 3.6 Bagi mengoptimumkan sumber dan mengelakkan pertindihan tugas, fungsi berkaitan keselamatan siber sektor awam yang sebelum ini dikendalikan oleh Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) telah diserahkan kepada NACSA, termasuklah peranan dan tanggungjawab [*Government Computer Emergency Response Team (GCERT)*].

#### 4. JENIS-JENIS INSIDEN KESELAMATAN SIBER

- 4.1 Jenis-jenis insiden keselamatan siber adalah seperti yang berikut:

- (i) **Penafian Perkhidmatan (*Denial of Service, DoS*)**  
**atau Penafian Perkhidmatan Teragih (*Distributed Denial of Service, DDoS*)**

Serangan DoS atau DDoS merupakan serangan terhadap sistem atau rangkaian komputer yang menyebabkan ketidakupayaan sistem atau rangkaian tersebut untuk memberikan perkhidmatan kepada pengguna.



(ii) **Pencerobohan (*Intrusion*)**

Pencerobohan merujuk kepada capaian tanpa kebenaran/tidak sah yang berjaya menembusi sistem atau rangkaian. Insiden ini boleh mengakibatkan akaun pentadbir sistem diambil alih, laman web diceroboh, kerosakan pada sistem, data atau konfigurasi sistem dipinda dan/atau pemasangan kod hasad seperti *backdoor* atau *trojan*.

(iii) **Jangkitan Perisian Hasad (*Malicious Software, Malware*)**

Perisian hasad adalah perisian yang direka untuk memasuki sistem komputer tanpa kebenaran dan berpotensi membahayakan mesin atau rangkaian.

(iv) **Pengehosan Perisian Hasad (*Malware Hosting*)**

Pengehosan perisian hasad merujuk kepada keadaan di mana perisian hasad berada di dalam pelayan atau komputer pengguna secara tidak sah; seterusnya dijadikan sebagai sumber untuk dimuat turun atau diakses oleh siri serangan perisian hasad yang lain.

(v) **Percubaan Pencerobohan (*Intrusion Attempt*)**

Percubaan dengan hasrat untuk menceroboh atau mengambil alih sistem secara tidak sah melalui aktiviti imbasan *port* rangkaian, akses sistem secara *brute force* atau mengenal pasti kerentanan sistem.

(vi) **Potensi Serangan (*Potential Attack*)**

Potensi serangan adalah ancaman yang berkemungkinan berlaku akibat daripada kerentanan yang terdapat pada sistem/rangkaian atau kelemahan pada proses kerja sesebuah agensi. Serangan ini boleh memusnah, mendedah, meminda, melumpuh, mencuri atau mendapatkan akses yang tidak sah bagi tujuan menggunakan aset yang tidak dibenarkan. Serangan ini dikenal pasti berdasarkan maklumat risikan atau hasil pemantauan terhadap agensi.

## **5. TAHAP KEUTAMAAN TINDAKAN TERHADAP INSIDEN KESELAMATAN SIBER**

5.1 Tindakan terhadap insiden keselamatan siber yang berlaku hendaklah dibuat berasaskan kepada keseriusan sesuatu insiden. Tahap keutamaan tindakan terhadap insiden keselamatan siber akan ditentukan seperti yang berikut:

- (i) **Keutamaan 1** – insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan Kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu.
- (ii) **Keutamaan 2** – insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1.

- 5.2 Sekiranya berstatus Keutamaan 1, agensi hendaklah melaporkan insiden kepada NC4 bagi tujuan penyelarasan dan memaklumkan kepada agensi yang menyeliaanya dalam tempoh 24 jam selepas insiden dikesan serta mengaktifkan Pelan Kesyinambungan Perkhidmatan (Business Continuity Plan, BCP) dan Pelan Pemulihan Bencana (Disaster Recovery Plan, DRP) sekiranya perlu.
- 5.3 Bagi Keutamaan 2, agensi hendaklah melaksanakan pengendalian insiden secara sendiri dan seterusnya memaklumkan kepada NC4 dan agensi yang menyeliaanya setelah proses pengendalian insiden dan pemulihan pada peringkat agensi selesai.

## **6. PENUBUHAN CSIRT AGENSI**

- 6.1 Ketua Agensi hendaklah menubuhkan CSIRT Agensi dan menyelaraskan penubuhan CSIRT Agensi di bawah seliaannya mengikut keperluan. Bagi agensi yang tiada keperluan untuk menubuhkan CSIRT, agensi tersebut hendaklah melaporkan terus kepada CSIRT Agensi yang menyeliaanya.
- 6.2 Sebagai langkah mengukuhkan pengurusan dan pengendalian keselamatan siber sektor awam serta memastikan insiden ditangani dengan berkesan, setiap agensi hendaklah:
- (i) Menubuhkan CSIRT atau yang setara dengannya bagi menangani insiden keselamatan siber.

- (ii) CSIRT Agensi bertindak sebagai *first level support* kepada NC4 dalam mengendalikan insiden keselamatan siber, mengawasi dan memberi khidmat nasihat berkaitan keselamatan siber kepada agensi di bawah seliaannya.
- (iii) bertanggungjawab melaporkan insiden keselamatan siber kepada Ketua Pegawai Digital (Chief Digital Officer, CDO) atau yang setara dan bersesuaian dengan struktur agensi masing-masing.

6.3 Dua model struktur pewujudan CSIRT Agensi sektor awam adalah dicadangkan seperti yang berikut:

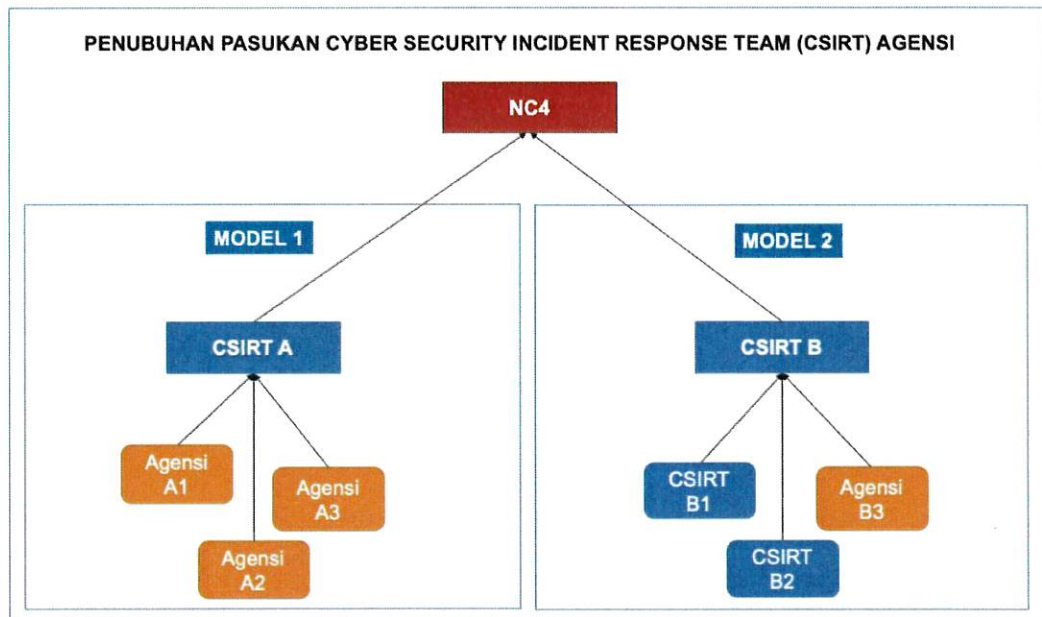
(i) **Model 1**

CSIRT ditubuhkan hanya pada peringkat Ketua Agensi yang mana agensi di bawah seliaannya tidak mempunyai CSIRT. CSIRT ini bertanggungjawab terhadap insiden yang berlaku di agensi seliaannya.

(ii) **Model 2**

CSIRT ditubuhkan pada peringkat Ketua Agensi dan juga agensi di bawahnya. CSIRT Agensi di bawahnya bertanggungjawab atas insiden masing-masing dan perlu diselaraskan pada peringkat Ketua Agensi.

6.4 Cadangan struktur kedua-dua model adalah seperti yang berikut:



Rajah 1 Struktur Model CSIRT Agensi Sektor Awam

6.5 Cadangan struktur kedua-dua model adalah seperti yang berikut:

| Peranan        | Pegawai Bertanggungjawab   | Tugas dan Tanggungjawab   |
|----------------|--|---|
| Pengarah CSIRT | Ketua Pegawai Digital (Chief Digital Officer, CDO)/Pengurus ICT atau yang setara | <ul style="list-style-type: none"> <li>• Menguruskan tindakan insiden yang berlaku sehingga keadaan pulih.</li> <li>• Mengaktifkan BCP/DRP jika perlu.</li> <li>• Menentukan sama ada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang/keselamatan.</li> </ul> |

|                |  |   |
|----------------|--|---|
| Pengurus CSIRT | Pegawai Keselamatan ICT (ICTSO) atau yang setara               | <ul style="list-style-type: none"> <li>• Menentukan tahap keutamaan insiden.</li> <li>• Melaporkan insiden kepada Pengarah CSIRT.</li> <li>• Mengambil langkah pemulihan awal.</li> </ul> |
| Ahli CSIRT     | Pegawai Teknologi Maklumat/Penolong Pegawai Teknologi Maklumat | <ul style="list-style-type: none"> <li>• Mengendalikan insiden berdasarkan panduan yang telah ditetapkan.</li> </ul>  |

Jadual 1 Keahlian dan Tanggungjawab CSIRT Agensi

6.6 Keahlian CSIRT Agensi boleh dilantik daripada kalangan pegawai sedia ada yang mengendalikan keselamatan maklumat, rangkaian, operasi sistem atau mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.

## 7. PEMAKLUMAN PENUBUHAN DAN PENGEMASKINIAN MAKLUMAT CSIRT AGENSI KEPADA NC4

7.1 Agensi hendaklah memaklumkan maklumat CSIRT Agensi kepada NC4 bagi tujuan rekod dan penyelarasan. Bagi agensi yang baru menubuhkan CSIRT, pemakluman kepada NC4 hendaklah dibuat menggunakan Borang CSIRT01 – Borang Pelantikan CSIRT Agensi seperti di **Lampiran A**.

7.2 Sebarang pertukaran ahli CSIRT Agensi juga hendaklah dimaklumkan kepada NC4 dengan kadar segera menggunakan Borang CSIRT02 – Borang Kemaskini Maklumat Ahli CSIRT Agensi seperti di **Lampiran B**.

## **8. TANGGUNGJAWAB CSIRT AGENSI**

8.1 Tanggungjawab CSIRT Agensi meliputi semua bidang tugas pengurusan dan pengendalian insiden keselamatan siber termasuklah agensi di bawah seliaannya seperti yang berikut:

- (i) Memantau, mengesan insiden, menerima, dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber.
- (ii) Merekod dan menjalankan siasatan awal terhadap insiden yang diterima.
- (iii) Melaksanakan pengurusan dan pengendalian insiden keselamatan siber serta mengambil tindakan awal pemulihan.
- (iv) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan.

- (v) Melaporkan insiden keselamatan siber kepada agensi yang menyeliaanya (sekiranya ada) dan NC4.
- (vi) Menasihati agensi di bawah seliaannya mengambil tindakan pemulihan dan pengukuhan.
- (vii) Menyebarkan makluman/amaran berkaitan insiden kepada agensi lain di bawah seliaannya.
- (viii) Memastikan fail log disimpan sekurang-kurangnya enam bulan di tempat yang selamat.

8.2 Apabila berlakunya insiden keselamatan siber, pengarah CSIRT Agensi hendaklah menggerakkan ahli CSIRT Agensi untuk mengambil tindakan seperti yang berikut:

- (i) Mengurus dan mengambil tindakan terhadap insiden yang berlaku sehingga keadaan pulih.
- (ii) Mengaktifkan BCP dan/atau DRP jika perlu.
- (iii) Melapor dan memaklumkan insiden keselamatan siber kepada NC4 serta agensi yang menyeliaanya.
- (iv) Menentukan sama ada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang.



## **9. TANGGUNGJAWAB KETUA JABATAN**

Ketua Jabatan hendaklah memastikan kementerian/jabatan dan agensi di bawah seliaannya mematuhi garis panduan pengurusan insiden keselamatan, akta, peraturan, dan prosedur berkaitan keselamatan siber yang masih berkuat kuasa.

## **10. TANGGUNGJAWAB NC4 DALAM PENGURUSAN DAN PENGENDALIAN INSIDEN SIBER SEKTOR AWAM**

10.1 Tanggungjawab NC4 dalam pengurusan dan pengendalian insiden keselamatan siber adalah seperti yang berikut:

- (i) Menyedia dan menyebarkan *alert and advisory* kepada CSIRT Agensi sekiranya terdapat potensi serangan siber.
- (ii) Menyediakan khidmat nasihat kepada CSIRT Agensi berkaitan pengurusan dan pengendalian insiden keselamatan siber.
- (iii) Menyelaras pengurusan dan pengendalian insiden pada peringkat agensi serta memberi nasihat berkenaan tindakan pemulihan dan pengukuhan.
- (iv) Menyelaras program pertukaran dan perkongsian maklumat bersama CSIRT Agensi.

- (v) Menyediakan laporan statistik insiden keselamatan siber kepada pihak pengurusan NACSA dan MKN, JPM.
- (vi) Menyediakan input situasi keselamatan siber kepada pihak pengurusan MKN, JPM.
- (vii) Mengumpul dan mengemas kini maklumat CSIRT Agensi.
- (viii) Mengadakan mesyuarat penyelarasan CSIRT, sesi perkongsian ilmu (technology update), latihan, dan kursus kepada CSIRT Agensi.

## **11. CARTA ALIRAN PROSES KERJA PELAPORAN INSIDEN DAN PROSEDUR OPERASI STANDARD PENGURUSAN DAN PENGENDALIAN INSIDEN KESELAMATAN SIBER SEKTOR AWAM**

11.1 Carta Aliran Proses Kerja Pelaporan Insiden Keselamatan Siber CSIRT Agensi dijelaskan dalam **Lampiran C**.

11.2 Prosedur Operasi Standard Pengurusan dan Pengendalian Insiden Keselamatan Siber CSIRT Agensi dijelaskan dalam **Lampiran D**.

## **12. MEKANISME PELAPORAN INSIDEN**

Pelaporan insiden keselamatan siber kepada NC4 boleh dibuat melalui borang dalam talian yang disediakan di laman web <https://www.nacsa.gov.my>.

### **13. ARAHAN DAN PROSEDUR PENGURUSAN KESELAMATAN SIBER NEGARA**

13.1 Bagi agensi yang telah dikategorikan sebagai CNII, pengendalian insiden semasa krisis siber negara hendaklah turut merujuk kepada Arahan Majlis Keselamatan Negara No. 26: Pengurusan Keselamatan Siber Negara tahun 2021 dan Prosedur Tindak Balas, Komunikasi dan Penyelarasan Pengurusan Krisis Siber Negara.

13.2 Semua agensi hendaklah mematuhi sebarang arahan yang dikeluarkan oleh NACSA dan MKN, JPM dari semasa ke semasa berkaitan pengurusan keselamatan siber negara.

### **14. PEMAKAIAN**

Pekeliling ini terpakai kepada semua agensi Perkhidmatan Awam Persekutuan bermula dari tarikh pekeliling ini ditandatangani. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, peruntukan Pekeliling Am ini pada keseluruhannya dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Negeri dan Pihak Berkuasa Tempatan.

### **15. PEMBATALAN**

15.1 Dengan berkuat kuasanya Pekeliling Am ini, pekeliling dan surat pekeliling yang berikut adalah dibatalkan:

- (i) Pekeliling Am Bil. 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT).
- (ii) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam.
- (iii) Surat Arahan Ketua Pengarah MAMPU bertarikh 23 Mac 2009 - Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi Kerajaan.

## **16. MAKLUMAT PERHUBUNGAN DAN KHIDMAT NASIHAT**

16.1 Sebarang kemusykilan berkaitan dengan Pekeliling Am ini hendaklah dirujuk kepada NC4 melalui maklumat perhubungan seperti di bawah:

### **Pusat Penyelarasan dan Kawalan Siber Negara (NC4)**

Agensi Keselamatan Siber Negara (NACSA)

Majlis Keselamatan Negara

Aras LG & G, Blok Barat

Bangunan Perdana Putra

62502 PUTRAJAYA

No. Telefon: 03-8064 4888

No. Faks: 03-8064 4848

E-mel: [admin@nacs.gov.my](mailto:admin@nacs.gov.my)

16.2 Khidmat nasihat berkaitan insiden keselamatan siber boleh diperoleh pada setiap hari bekerja Isnin hingga Jumaat (kecuali cuti am) mulai jam 9.00 pagi hingga 6.00 petang melalui saluran berikut:

No. Telefon: 03-8064 4888

E-mel: [cert@nc4.gov.my](mailto:cert@nc4.gov.my)

16.3 Sekiranya agensi menghadapi insiden keselamatan siber yang kritikal, iaitu insiden di bawah **Keutamaan 1** seperti di perenggan 5.1 (a), NC4 boleh dihubungi serta merta. Jika berlaku di luar waktu pejabat, nombor telefon yang boleh dihubungi ialah **03-8064 4884 (24 jam, 7 hari seminggu)**.

**“BERKHIDMAT UNTUK NEGARA”**



**(TAN SRI DATO' SERI MOHD ZUKI BIN ALI)**

Ketua Setiausaha Negara



**BORANG PENUBUHAN DAN PELANTIKAN  
COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) AGENSI**



**MAKLUMAT CSIRT AGENSI**

Nama CSIRT Agensi : \_\_\_\_\_  
Kementerian / Kerajaan Negeri : \_\_\_\_\_  
Jabatan / Badan Berkanun / Agensi : \_\_\_\_\_  
Alamat : \_\_\_\_\_  
No. Tel. : \_\_\_\_\_ No. Faks : \_\_\_\_\_  
Tarikh Penubuhan : \_\_\_\_\_ Ruj. Kelulusan : \_\_\_\_\_  
E-mel CSIRT Agensi : \_\_\_\_\_

**MAKLUMAT PENGARAH CSIRT**

Nama : \_\_\_\_\_  
No. Kad Pengenalan: \_\_\_\_\_  
Jawatan : \_\_\_\_\_ Gred : \_\_\_\_\_  
\*Peranan : CIO / CISO / Pengurus ICT / Lain-lain  
No. Tel. Pejabat : \_\_\_\_\_ No. Tel. Bimbit : \_\_\_\_\_  
E-mel : \_\_\_\_\_

**MAKLUMAT PENGURUS CSIRT**

Nama : \_\_\_\_\_  
No. Kad Pengenalan: \_\_\_\_\_  
Jawatan : \_\_\_\_\_ Gred : \_\_\_\_\_  
\*Peranan : ICTSO / Pengurus ICT  
No. Tel. Pejabat : \_\_\_\_\_ No. Tel. Bimbit : \_\_\_\_\_  
E-mel : \_\_\_\_\_

**MAKLUMAT AHLI CSIRT**

Nama : \_\_\_\_\_  
No. Kad Pengenalan: \_\_\_\_\_  
Jawatan : \_\_\_\_\_ Gred : \_\_\_\_\_  
\*Peranan : Pentadbir Sistem Aplikasi / Pentadbir Keselamatan / Pentadbir Rangkaian /  
Pentadbir Server / Pentadbir Laman Web / Pentadbir E-mel / Pentadbir  
Pangkalan Data / Pentadbir Aset ICT / Pentadbir Pusat Data  
No. Tel. Pejabat : \_\_\_\_\_ No. Tel. Bimbit : \_\_\_\_\_  
E-mel : \_\_\_\_\_  
\*\*Nama Agensi : \_\_\_\_\_



**BORANG PENUBUHAN DAN PELANTIKAN  
COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) AGENSI**



|                     |   |   |
|---------------------|---|---|
| Nama                | : | _____   |
| No. Kad Pengenalan: |   | _____   |
| Jawatan             | : | _____ Gred : _____  |
| *Peranan            | : | Pentadbir Sistem Aplikasi / Pentadbir Keselamatan / Pentadbir Rangkaian /<br>Pentadbir Server / Pentadbir Laman Web / Pentadbir E-mel / Pentadbir<br>Pangkalan Data / Pentadbir Aset ICT / Pentadbir Pusat Data |
| No. Tel. Pejabat    | : | _____ No. Tel. Bimbit : _____   |
| E-mel               | : | _____   |
| **Nama Agensi       | : | _____   |
|                     |   |   |
| Nama                | : | _____   |
| No. Kad Pengenalan: |   | _____   |
| Jawatan             | : | _____ Gred : _____  |
| *Peranan            | : | Pentadbir Sistem Aplikasi / Pentadbir Keselamatan / Pentadbir Rangkaian /<br>Pentadbir Server / Pentadbir Laman Web / Pentadbir E-mel / Pentadbir<br>Pangkalan Data / Pentadbir Aset ICT / Pentadbir Pusat Data |
| No. Tel. Pejabat    | : | _____ No. Tel. Bimbit : _____   |
| E-mel               | : | _____   |
| **Nama Agensi       | : | _____   |
|                     |   |   |
| Nama                | : | _____   |
| No. Kad Pengenalan: |   | _____   |
| Jawatan             | : | _____ Gred : _____  |
| *Peranan            | : | Pentadbir Sistem Aplikasi / Pentadbir Keselamatan / Pentadbir Rangkaian /<br>Pentadbir Server / Pentadbir Laman Web / Pentadbir E-mel / Pentadbir<br>Pangkalan Data / Pentadbir Aset ICT / Pentadbir Pusat Data |
| No. Tel. Pejabat    | : | _____ No. Tel. Bimbit : _____   |
| E-mel               | : | _____   |
| **Nama Agensi       | : | _____   |





**BORANG PENUBUHAN DAN PELANTIKAN  
COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) AGENSI**



**PENGESAHAN KETUA JABATAN/KETUA PEGAWAI MAKLUMAT (CIO)**

Nama : \_\_\_\_\_

Jawatan : \_\_\_\_\_

No. Tel. Pejabat: \_\_\_\_\_ No. Faks : \_\_\_\_\_

Tandatangan : \_\_\_\_\_ Tarikh : \_\_\_\_\_

Borang yang telah lengkap hendaklah dikemukakan ke alamat seperti berikut :-

Agensi Keselamatan Siber Negara (NACSA)  
Majlis Keselamatan Negara  
Aras LG & G, Blok Barat  
Bangunan Perdana Putra  
Pusat Pentadbiran Kerajaan Persekutuan  
62502 PUTRAJAYA

**Atau melalui:**

No. Faks – 03-8064 4848

E-mel – [daftarcsirt@nacsa.gov.my](mailto:daftarcsirt@nacsa.gov.my) (borang yang lengkap dan diimbas)

**NOTA:**

\* Peranan – Pilih yang berkaitan

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





**BORANG KEMASKINI MAKLUMAT AHLI  
COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) AGENSI**



**MAKLUMAT CSIRT AGENSI**

Nama CSIRT Agensi : \_\_\_\_\_  
Kementerian / Kerajaan Negeri : \_\_\_\_\_  
Jabatan / Badan Berkanun / Agensi : \_\_\_\_\_  
E-mel Kumpulan (group e-mail) : \_\_\_\_\_

**MAKLUMAT PENGARAH CSIRT YANG BAHARU (MENGANTIKAN PENGARAH CSIRT YANG LAMA)**

Nama : \_\_\_\_\_  
No. K/P. : \_\_\_\_\_  
Jawatan : \_\_\_\_\_ Gred : \_\_\_\_\_  
\*Peranan : CIO / CISO / lain-lain  
No. Tel. Pejabat : \_\_\_\_\_ No. Tel. Bimbit : \_\_\_\_\_  
E-mel : \_\_\_\_\_

**MAKLUMAT PENGURUS CSIRT YANG BAHARU (MENGANTIKAN PENGURUS CSIRT YANG LAMA)**

Nama : \_\_\_\_\_  
No. K/P : \_\_\_\_\_  
Jawatan : \_\_\_\_\_ Gred : \_\_\_\_\_  
\*Peranan : ICTSO / Lain-lain  
No. Tel. Pejabat : \_\_\_\_\_ No. Tel. Bimbit : \_\_\_\_\_  
E-mel : \_\_\_\_\_

**MAKLUMAT AHLI CSIRT YANG BERTUKAR**

Nama : \_\_\_\_\_  
No. K/P : \_\_\_\_\_  
Jawatan : \_\_\_\_\_ Gred : \_\_\_\_\_  
No. Tel. Pejabat : \_\_\_\_\_ No. Tel. Bimbit : \_\_\_\_\_  
E-mel : \_\_\_\_\_  
Tarikh Bertukar : \_\_\_\_\_  
Tempat ditukarkan : \_\_\_\_\_



**BORANG KEMASKINI MAKLUMAT AHLI  
COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) AGENSI**



|                   |   |                               |
|-------------------|---|-------------------------------|
| Nama              | : | _____                         |
| No. K/P.          | : | _____                         |
| Jawatan           | : | _____ Gred : _____            |
| No. Tel. Pejabat  | : | _____ No. Tel. Bimbit : _____ |
| E-mel             | : | _____                         |
| Tarikh bertukar   | : | _____                         |
| Tempat ditukarkan | : | _____                         |
|                   |   |                               |
| Nama              | : | _____                         |
| No. K/P.          | : | _____                         |
| Jawatan           | : | _____ Gred : _____            |
| No. Tel. Pejabat  | : | _____ No. Tel. Bimbit : _____ |
| E-mel             | : | _____                         |
| Tarikh bertukar   | : | _____                         |
| Tempat ditukarkan | : | _____                         |

**MAKLUMAT PENAMBAHAN AHLI CSIRT BAHARU**

|                  |   |   |
|------------------|---|---|
| Nama             | : | _____   |
| No. K/P.         | : | _____   |
| Jawatan          | : | _____ Gred : _____  |
| *Peranan         | : | Pentadbir Sistem Aplikasi / Pentadbir Keselamatan / Pentadbir Rangkaian /<br>Pentadbir Server / Pentadbir Laman Web / Pentadbir E-mel /<br>Pentadbir Pangkalan Data / Pentadbir Pusat Data / Pentadbir Aset ICT |
| No. Tel. Pejabat | : | _____ No. Tel. Bimbit : _____   |
| E-mel            | : | _____   |
| **Nama Agensi    | : | _____   |
|                  |   |   |
| Nama             | : | _____   |
| No. K/P.         | : | _____   |
| Jawatan          | : | _____ Gred : _____  |
| *Peranan         | : | Pentadbir Sistem Aplikasi / Pentadbir Keselamatan / Pentadbir Rangkaian /<br>Pentadbir Server / Pentadbir Laman Web / Pentadbir E-mel /<br>Pentadbir Pangkalan Data / Pentadbir Pusat Data / Pentadbir Aset ICT |
| No. Tel. Pejabat | : | _____ No. Tel. Bimbit : _____   |
| E-mel            | : | _____   |
| **Nama Agensi    | : | _____   |



**BORANG KEMASKINI MAKLUMAT AHLI  
COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) AGENSI**



|                  |   |   |
|------------------|---|---|
| Nama             | : | _____   |
| No. K/P          | : | _____   |
| Jawatan          | : | _____ Gred : _____  |
| *Peranan         | : | Pentadbir Sistem Aplikasi / Pentadbir Keselamatan / Pentadbir Rangkaian /<br>Pentadbir Server / Pentadbir Laman Web / Pentadbir E-mel /<br>Pentadbir Pangkalan Data / Pentadbir Pusat Data / Pentadbir Aset ICT |
| 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 yang telah lengkap hendaklah dikemukakan ke alamat seperti berikut :-

Agensi Keselamatan Siber Negara (NACSA)  
Majlis Keselamatan Negara  
Aras LG & G, Blok Barat  
Bangunan Perdana Putra  
Pusat Pentadbiran Kerajaan Persekutuan  
62502 PUTRAJAYA

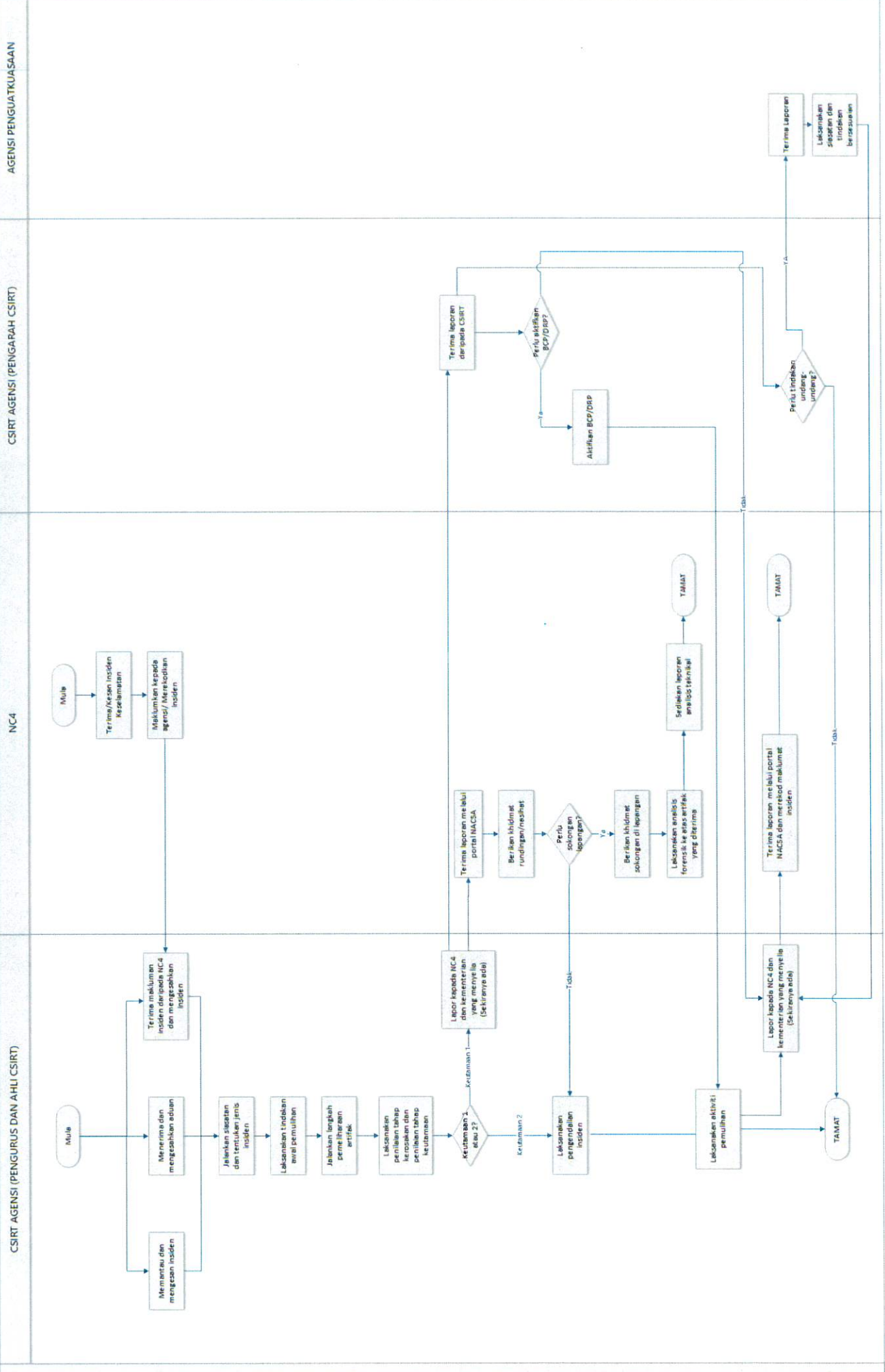
**Atau melalui:**

No. Faks – 03-8064 4848  
E-mel – [daftarcsirt@nacsa.gov.my](mailto:daftarcsirt@nacsa.gov.my) (borang yang lengkap dan diimbas)

**NOTA:**

- \* Peranan – Pilih yang berkaitan
- \*\* Tuliskan nama agensi sekiranya berlainan dengan yang dinyatakan dalam ruangan Maklumat CSIRT Agensi

CARTA ALIRAN PROSES PELAPORAN INSIDEN KESELAMATAN SIBER SEKTOR AWAM



**LAMPIRAN D**

**PROSEDUR OPERASI STANDARD  
PENGURUSAN PENGENDALIAN INSIDEN AGENSI SEKTOR AWAM**



## SENARAI KANDUNGAN

|  |    |
|--|----|
| 1. OBJEKTIF .....  | 31 |
| 2. PENGENALAN.....   | 31 |
| 3. PROSEDUR OPERASI STANDARD.....                                | 33 |
| A. Pentadbiran.....  | 33 |
| B. Pengurusan dan Pengendalian Insiden .....                     | 34 |
| C. Proses Kerja Pengendalian Insiden .....                       | 35 |
| D. Penyebaran Maklumat.....                                      | 36 |
| E. Penyelarasan Pengurusan Insiden Keselamatan Siber .....       | 36 |
| 4. SENARAI TEMPLAT.....  | 37 |
| A. TEMPLAT SENARAI SEMAK PENGENDALIAN INSIDEN .....              | 37 |
| B. TEMPLAT BORANG PENGENDALIAN INSIDEN<br>KESELAMATAN SIBER..... | 39 |
| C. TEMPLAT LAPORAN ANALISIS FAIL LOG .....                       | 42 |
| D. TEMPLAT LAPORAN KRONOLOGI INSIDEN KESELAMATAN<br>SIBER.....   | 43 |
| 5. SINGKATAN PERKATAAN .....                                     | 44 |

# **GARIS PANDUAN PENGURUSAN DAN PENGENDALIAN INSIDEN KESELAMATAN SIBER**

## **1. OBJEKTIF**

Dokumen ini menerangkan prosedur yang diguna pakai oleh CSIRT Agensi bagi mengendalikan insiden keselamatan siber di agensi masing-masing dan agensi di bawah seliaannya.

## **2. PENGENALAN**

Secara amnya, tanggungjawab CSIRT Agensi meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan siber yang dialami oleh agensi itu sendiri dan/atau agensi di bawah seliaannya. Bidang tugas adalah seperti yang berikut:

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

- i. Merekod aduan.
- ii. Mengemas kini maklumat insiden.
- iii. Menyelenggara fail data insiden untuk membantu kelancaran operasi CSIRT Agensi.

### **b) Pengurusan dan Pengendalian Insiden Keselamatan Siber**

Tugas pengendalian insiden dijalankan apabila aduan diterima sehingga kes insiden selesai dikendalikan. Bidang tugas ini meliputi proses berikut:

- i. Penerimaan laporan/aduan insiden.
- ii. Penyiasatan kes.
- iii. Pengendalian insiden.
- iv. Penyediaan laporan selepas pengendalian.
- v. Khidmat nasihat kepada agensi terlibat.

c) Penyebaran Maklumat

Setiap CSIRT Agensi mestilah menyebarkan maklumat berkaitan insiden keselamatan siber dari semasa ke semasa kepada agensi-agensi di bawah seliaannya bagi berkongsi maklumat untuk meningkatkan tahap keselamatan siber agensi dan membendung insiden keselamatan siber sektor awam.

Penyebaran maklumat dilakukan secara reaktif bagi insiden yang telah berlaku dan secara proaktif mengenai kerentanan serta ancaman yang bakal melanda agensi supaya tindakan pengukuhan dilakukan untuk mengelakkan insiden kepada agensi di bawah seliaannya.

d) Penyelarasan Pengurusan dan Pengendalian Insiden

CSIRT Agensi berperanan menyelaraskan mesyuarat pengurusan dan pengendalian insiden keselamatan siber antara agensi di bawah seliaannya serta pihak lain yang terlibat dalam pengendalian insiden keselamatan siber. Agenda utama mesyuarat adalah untuk berkongsi maklumat bagi meningkatkan tahap keselamatan siber dan membendung kejadian insiden keselamatan siber antara agensi di bawah seliaannya serta sektor awam amnya.



### 3. PROSEDUR OPERASI STANDARD

#### Proses Pengurusan dan Pengendalian Insiden Keselamatan Siber

##### A. Pentadbiran

| Tanggungjawab | Keterangan Aktiviti  | Pegawai Yang Dirujuk |
|---------------|--|----------------------|
| Ahli CSIRT    | Terima dan rekod maklumat awal insiden menggunakan Borang Pengendalian Insiden Keselamatan Siber       | Agensi yang terlibat |
|               | Simpan dan kemas kini maklumat/dokumen yang berkaitan dengan mengambil kira tahap klasifikasi maklumat |                      |
|               | kemas kini maklumat insiden semasa/selepas siasatan  |                      |

## B. Pengurusan dan Pengendalian Insiden

| <b>Tanggungjawab</b>         | <b>Keterangan Aktiviti</b>                                    | <b>Pegawai Yang Dirujuk</b> |
|------------------------------|---|-----------------------------|
| Pengurus CSIRT<br>Ahli CSIRT | Memantau, mengesan insiden, menerima, dan mengesahkan insiden | Agensi yang terlibat        |
| Pengurus CSIRT<br>Ahli CSIRT | Jalankan siasatan awal insiden dan tentukan jenis insiden     | Agensi yang terlibat        |
| Pengurus CSIRT<br>Ahli CSIRT | Laksanakan tindakan awal pemulihan                            | Agensi yang terlibat        |
| Ahli CSIRT                   | Dapatkan dan pelihara artifak terlibat                        | Agensi yang terlibat        |
| Pengurus CSIRT<br>Ahli CSIRT | Laksanakan penilaian tahap kerosakan dan tahap keutamaan      | Agensi yang terlibat        |
| Pengurus CSIRT<br>Ahli CSIRT | Tentukan sekiranya perlu aktifkan BCP/DRP                     | Pengarah CSIRT              |
| Ahli CSIRT                   | Laporkan insiden kepada NC4 (jika Keutamaan 1)                | NC4                         |

### C. Proses Kerja Pengendalian Insiden

| Tanggungjawab | Keterangan Aktiviti  | Pegawai Yang Dirujuk   |
|---------------|--|--|
| Ahli CSIRT    | Mengadakan Mesyuarat Pengurusan  | Pengurus CSIRT   |
|               | Jalankan Siasatan Lanjut/ Mesyuarat/Perbincangan                                 | Agensi yang terlibat   |
|               | Melakukan analisis artifak dan pembentangan hasil analisis                       | <ul style="list-style-type: none"> <li>● Pengurus CSIRT</li> <li>● Agensi yang terlibat</li> </ul> |
|               | Penyediaan Laporan Analisis Insiden Keselamatan Siber termasuk kronologi insiden | Agensi yang terlibat   |
|               | Jalankan proses/tindakan pemulihan   | Agensi yang terlibat   |
|               | Tentukan sekiranya perlu tindakan undang-undang                                  | Pengarah CSIRT   |
|               | Penutupan Kes Insiden  | Agensi yang terlibat   |
|               | kemas kini Maklumat dan Status Insiden   | Agensi yang terlibat   |
|               | Maklumkan insiden kepada NC4 (jika Keutamaan 2)                                  | NC4  |

#### D. Penyebaran Maklumat

| <b>Tanggungjawab</b> | <b>Keterangan Aktiviti</b>                           | <b>Pegawai Yang Dirujuk</b> |
|----------------------|--|-----------------------------|
| Ahli CSIRT           | Dapatkan maklumat dari Internet atau agensi lain     | Agensi yang terlibat        |
|                      | Kajian terperinci terhadap ancaman dan impak insiden | Agensi yang terlibat        |
|                      | Sediakan nota makluman mengenai ancaman              | Pengurus CSIRT              |
|                      | Sebar nota makluman kepada agensi                    | Agensi yang terlibat        |

#### E. Penyelarasan Pengurusan Insiden Keselamatan Siber

| <b>Tanggungjawab</b> | <b>Keterangan Aktiviti</b>                                     | <b>Pegawai Yang Dirujuk</b>   |
|----------------------|--|---|
| Ahli CSIRT           | Mengadakan mesyuarat penyelarasan insiden siber secara berkala | <ul style="list-style-type: none"><li>● Pengurus CSIRT</li><li>● Agensi yang terlibat</li></ul> |

#### 4. SENARAI TEMPLAT

##### A. TEMPLAT SENARAI SEMAK PENGENDALIAN INSIDEN

| SENARAI SEMAK PENGENDALIAN INSIDEN |  |                          |         |
|------------------------------------|--|--------------------------|---------|
| Bil                                | Tindakan   | Tanda (√)                | Catatan |
| 1.                                 | Hubungi agensi yang terlibat dengan insiden.   | <input type="checkbox"/> |         |
| 2.                                 | Dapatkan maklumat agensi, pegawai yang bertanggungjawab dan maklumat pegawai yang boleh dihubungi seperti nama, jawatan, nombor telefon, dan alamat e-mel.   | <input type="checkbox"/> |         |
| 3.                                 | Dapatkan keterangan mengenai insiden yang berlaku.   | <input type="checkbox"/> |         |
| 4.                                 | Dapatkan maklumat perisian dan perkakasan yang terlibat dengan insiden tersebut seperti nama sistem, alamat IP, fungsi sistem, <i>hostname</i> , pengguna terlibat, alamat IP DNS, jenis perisian, versi perisian dan bilangan server/komputer terlibat. | <input type="checkbox"/> |         |
| 5.                                 | Dapatkan maklumat tindakan awal yang telah diambil oleh agensi untuk menangani insiden tersebut.   | <input type="checkbox"/> |         |
| 6.                                 | Berikan khidmat nasihat kepada agensi untuk menghalang serangan dan tindakan seterusnya yang perlu dilaksanakan.   | <input type="checkbox"/> |         |

|     |   |                          |  |
|-----|---|--------------------------|--|
| 7.  | Kenal pasti tahap kerosakan dan tahap keutamaan dan melaksanakan tindakan berkaitan.              | <input type="checkbox"/> |  |
| 8.  | Tentukan sekiranya perlu mengaktifkan BCP/DRP.  | <input type="checkbox"/> |  |
| 9.  | Dapatkan dan pelihara artifak yang berkaitan dengan insiden.                                      | <input type="checkbox"/> |  |
| 10. | Laksanakan analisis kepada artifak.   | <input type="checkbox"/> |  |
| 11. | Menyedia dan membentangkan laporan hasil analisis dan cadangan pengukuhan kepada agensi terlibat. | <input type="checkbox"/> |  |
| 12. | Dapatkan maklum balas berkaitan tindakan pengukuhan yang dicadangkan.                             | <input type="checkbox"/> |  |
| 13. | Tentukan sekiranya perlu tindakan undang-undang.  | <input type="checkbox"/> |  |

**B. TEMPLAT BORANG PENGENDALIAN INSIDEN KESELAMATAN SIBER**

**CSIRT Agensi**  
**Alamat CSIRT agensi**  
**E-mel CSIRT agensi**

| <b>BORANG PENGENDALIAN INSIDEN KESELAMATAN SIBER</b>  |
|---|
| Tarikh dan Masa Dikesan:  |
| <b>Maklumat Agensi</b>  |
| Nama Pelapor:   |
| Nama Agensi:  |
| Alamat Penuh Agensi:  |
| No. Telefon Agensi:   |
| No. Faks:   |
| <b>Maklumat Insiden</b>   |
| Jenis Insiden:<br><input type="checkbox"/> DDoS<br><input type="checkbox"/> <i>Intrusion</i><br><input type="checkbox"/> <i>Malware Infection</i><br><input type="checkbox"/> <i>Malware Hosting</i><br><input type="checkbox"/> <i>Intrusion Attempt</i><br><input type="checkbox"/> <i>Potential Attack</i> |
| Tahap Keutamaan:<br><input type="checkbox"/> Keutamaan 1<br><input type="checkbox"/> Keutamaan 2  |
| Penerangan Mengenai Insiden:  |

| Indikasi Insiden:                                     |          |                      |
|---|----------|----------------------|
| <b>Maklumat Perkakasan dan Perisian yang Terlibat</b> |          |                      |
| Nama Sistem:  |          |                      |
| Domain:   |          |                      |
| Alamat IP DNS:  |          |                      |
| Maklumat Sistem yang Terkesan:                        |          |                      |
| Alamat IP   | Hostname | Sistem Pengoperasian |
|   |          |                      |
|   |          |                      |
|   |          |                      |
| Bilangan Hos Terkesan:                                |          |                      |
| <b>Maklumat Penyerang</b>                             |          |                      |
| Alamat IP Penyerang:                                  |          |                      |
| Keterangan Mengenai Penyerang:                        |          |                      |
| <b>Tindakan dan Pengesahan</b>                        |          |                      |



|  |
|--|
| Tindakan Awal yang Dilaksanakan oleh Agensi:   |
| Cadangan Tindakan Pengukuhan:  |
| Maklum Balas Berkaitan Tindakan Pengukuhan yang Dicadangkan:                                   |
| Tindakan Aktifkan BCP/DRP: <input type="checkbox"/> Perlu <input type="checkbox"/> Tidak Perlu |
| Tindakan Undang-Undang: <input type="checkbox"/> Perlu <input type="checkbox"/> Tidak Perlu    |
| Ulasan dan Pengesahan oleh Pengurus CSIRT:   |
| Tandatangan: <span style="float: right;">Cap:</span>   |

**C. TEMPLAT LAPORAN ANALISIS FAIL LOG**

**CSIRT Agensi**  
**Alamat CSIRT agensi**  
**E-mel CSIRT agensi**

**Nama Agensi :**

**Nama Fail Log :**

**No. Insiden :**

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

Rujukan Fail CSIRT agensi-Tarikh

**D. TEMPLAT LAPORAN KRONOLOGI INSIDEN KESELAMATAN SIBER**

**CSIRT Agensi**  
**Alamat CSIRT agensi**  
**E-mel CSIRT agensi**

**Nama Agensi :**

**Tarikh :**

**Lokasi :**

| <b>TARIKH</b> | <b>MASA</b> | <b>AKTIVITI</b> | <b>HASIL<br/>SIASATAN/PENEMUAN</b> |
|---------------|-------------|-----------------|------------------------------------|
|               |             |                 |                                    |
|               |             |                 |                                    |
|               |             |                 |                                    |
|               |             |                 |                                    |

Rujukan Fail CSIRT agensi-Tarikh

## **5. SINGKATAN PERKATAAN**

BCP - *Business Continuity Plan*

CSIRT - *Cyber Security Incident Response Team*

DRP - *Disaster Recovery Plan*

IP - *Internet Protocol*