BADAN SIBER &
SANDI NEGARA

PEMBENTUKAN CSIRT

DIREKTORAT PENANGGULANGAN DAN PEMULIHAN PEMERINTAH,
DEPUTI BIDANG PENANGGULANGAN DAN PEMULIHAN – BSSN

OUTLINE

- Tahapan pembentukan CSIRT
- Komponen CSIRT
- Deklarasi CSIRT
- Pendaftaran CSIRT

TAHAPAN PEMBENTUKAN CSIRT

Tahap 1 Edukasi Organisasi

Organisasi ingin membangun CSIRT namun belum memahami tentang CSIRT.

Tahap 2 Perencanaan

Organisasi memahami CSIRT dan mulai melakukan identifikasi dan analisis berbagai macam isu yang terkait penerapan CSIRT

Tahap 3 Penerapan

CSIRT dibentuk dan mulai menyelenggarakan layanan.

Tahap 4 Fase Operasional

CSIRT melakukan penanganan insiden

Tahap 5 Evaluasi

CSIRT menjadi Tim yang matang, mempunyai pengalaman melakukan penanganan insiden dan berkolaborasi dengan CSIRT lain

Source : Carnegie Mellon University

TAHAPAN PEMBENTUKAN CSIRT

Edukasi
- Memahami aturan hukum dan regul

Perencana
- Merumuskan Visi dan Misi
- Definisikan

Penerapan
- Memperoleh pendanaan
- Deklarasikan

Operasional
- Menjalankan layanan CSIRT
- Evaluasi

Kolaborasi
- Partisipasi pertukaran informasi
- Partisipasi

BADAN SIBER & SANDI NEGARA

KOMPONEN csirt

Konstituen

Siapa yang dilayani?

Resource

Resource apa yang dibutuhkan untuk melaksanakan misi?

Misi

Apa tujuan anda?

Prosedur dan Kebijakan

Prosedur dan kebijakan apa saja yang disiapkan?

Isu Organisasi

Bagaimana organisasi beroperasi?

Layanan

Layanan apa yang disediiakan?

Pendanaan

Bagaimana dukungan pembiayaan?

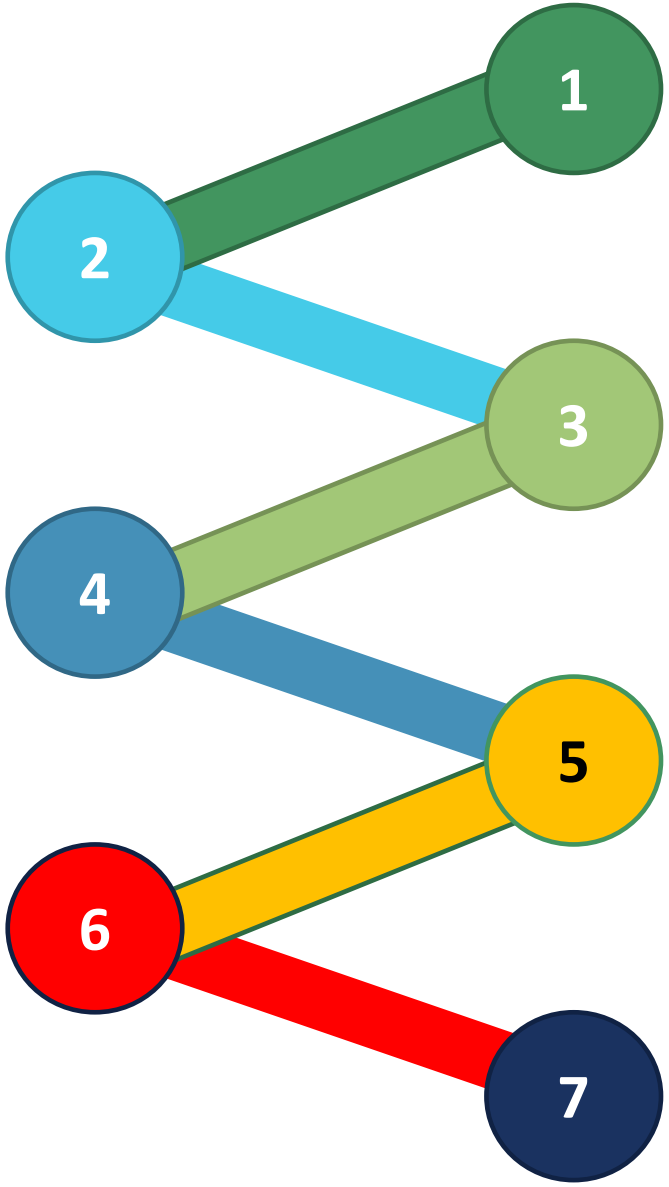
DEKLARASI csirt

Umumnya menggunakan RFC-2350

DEFINISI RFC 2350

- RFC adalah singkatan dari *Request for Comments*, yaitu seri dokumen informasi dan standar internet bernomor yang di ikuti secara luas oleh perangkat lunak untuk digunakan dalam jaringan, internet, dan beberapa sistem operasi jaringan, mulai dari Unix, Windows, dan Novell NetWare.
- RFC-2350 adalah standar yang dikeluarkan oleh IETF bulan Juni 1998 oleh N. Brownlee (Univ. of Auckland) dan E.Guttman (Sun Microsystem).
- Tujuan dokumen RFC-2350 untuk menggambarkan secara garis besar CSIRT, menyediakan informasi detail dalam suatu dokumen berformat legal, dimana konstituen dapat melihat kebijakan dan prosedur layanan CSIRT.
- Dokumen RFC-2350 dipublikasikan pada laman website CSIRT yang dibentuk.

RFC 2350



Document Information

Berisi informasi mengenai pembaruan versi dokumen, distribusi dan lokasi dokumen

Contact Information

Berisi informasi mengenai kontak tim baik alamat Email, Telepon maupun Time Zone

Charter

Berisi informasi mengenai Visi & Misi, Daftar Konstituen, Sponsorship dan Affiliation

Policies

Berisi informasi mengenai jenis insiden yang ditangani, metode koordinasi dan komunikasi

Services

Berisi informasi mengenai daftar layanan Tim CSIRT

Incident Reporting Form

Berisi informasi mengenai form pelaporan insiden

Disclaimer

Berisi mengenai hal-hal pernyataan penyangkalan

BADAN SIBER & SANDI NEGARA

RFC 2350 : Gov-CSIRT Indonesia

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi Gov-CSIRT Indonesia berdasarkan RFC 2350, yaitu informasi dasar mengenai Gov-CSIRT Indonesia, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi Gov-CSIRT Indonesia.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 8 Juli 2019.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Versi terbaru dari dokumen ini tersedia pada :
https://govcsirt.bssn.go.id/static/rfc2350/rfc2350-id.pdf (versi Bahasa Indonesia)
https://govcsirt.bssn.go.id/static/rfc2350/rfc2350-en.pdf (versi Bahasa Inggris)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) - Badan Siber dan Sandi Negara (BSSN). Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Kedua dokumen (versi bahasa inggris dan bahasa Indonesia) memiliki atribut yang sama, yaitu :

Judul : RFC 2350 Gov-CSIRT Indonesia;
Versi : 1.1;
Tanggal Publikasi : 8 Juli 2019;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2.1. Nama Tim

Government - Computer Security Incident Response Team (CSIRT) Indonesia
Disingkat : Gov-CSIRT Indonesia

2.2. Alamat

BSSN
Jl. Harsono RM No.70,
Ragunan - 12550
Pasar Minggu, Jakarta Sela
Indonesia

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

Telepon (021) 78833610

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak Ada

2.7. Alamat Surat Elektronik (*E-ma*

bantuan70[at]bssn.go.id

2.8. Kunci Publik (*Public Key*) dan Informasi/Data Enkripsi lain

Bits : 4096
ID : 0x73802BD6
Key Fingerprint : 1A35 DAEF E63B BE93 C314 3272 CE5D 2119 7380 2BD6

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBFtex4QBEADfLdjiJbwGTgOXUwyt/emyua3wIfYufUgpAKAzk2Dz8t9aj5bt
Co3adcXQw+5WnKSHbD7Q2VFUgLd+whIVuf6rAUraMcMrR10xWvvq2x4kEIEQiBXQ
CZOLgbN/9n+u2GqcD3x/XimyUDSN+I7DGh8+CioTWcahRQfcX70AqTlw5+VNFHT6
mrwAYfH8aQN2aPG+vW7j5K3AIEHVYFLYnU8F0FqBpcyFFIAWhqRgp6Jscsn9w0Ty
dR/v8laoaX1iE35XVyX3TXjS8TH+DCBuSP3BV0LVJJyISoEO4X0plKmERGW5UzaQ
CEbawtopt73QgWKcO5DTgMI247X3kekMchU8ENf25LdzrZ8znw8+DH/PggcCu6Hh
R/bccgXoFhQbrieZbDtuXKYn22/jJMWDKpJMQkGsPV2+qlMdYOXRrU87MhBE4dk2
dXLYCJki2qYnwddZp0HxRn6zznQ2VIrF+N3cBnQQB8izBFqcgy6gvkmJiUrGRn9n
upRryX7Wp1djfA13Veb1HftQNauOcWsJQt//fj5+MC9P6r3A4S2rgnojQv3zuPxP
XUVuvZOE0ywqXTfxPd7DdJE3ilP8fLvdWEZoFHlZkBkAZtFFsbjNlEhUc7IBQtOR
B7wRptGQxajH26ru/atRpcfxAFx6pfYG5Hr0X1a7xqmpvPdxFcs5dQ0NnwARAQAB
tDRCYW50dWFuNzAgUHVzb3Bza2Ftc2luYXMgQlNTTiA8YmFudHVhbjcwQGJzc24u
Z28uaWQ+iQJUBBMBCAA+FiEEGjXa7+Y7vpPDFDJyzl0hGXOAK9YFAltex4QCGyMF
CQlmAYAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQzl0hGXOAK9Y9lA/+NULC
uXxF+Ko/l3x482/7yJS6oElhqY17nskNFjmBqM6fwTFdQybarqs1AgxN3ne26MWs
8McEOEOZyGLngRWUwuhrKQI7okrxXhbQGMINdSQ1IuPw0Bx7aYsUWnEFqMOApLAB
2Zm7CqYfrwsNGp6sWAwimO+05AOvr7jcqeBfwYyfDImO0Rf75YjPU6yJ+4NyEUWE
JubnHIYk47fV4T6O7BjvdgHIYHe51qDKo6xxmt32Wcn05fzGxTaPcIgBC3krrwNB
vkPTTMDIkJ6fEBe5q476Xs+7RPRmIr4FE5tu7/GoVGKJCKIvXJWCZrYawhACjE8h
WGksMO/XgZgXAA1/KIIjfJUJ0rjPMjgktq23Zg==
=yC+0
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://bssn.go.id/wp-content/uploads/2018/08/Publik-Key-Bantuan70-pub.asc

3.1. Misi

Tujuan dari Gov-CSIRT Indonesia, yaitu :

a. membangun, mengoordinasikan, mengolaborasikan dan mengoperasionalkan sistem mitigasi, manajemen krisis, penanggulangan dan pemulihan terhadap insiden keamanan siber pada sektor pemerintah
b. membangun kerja sama dalam rangka penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah
c. membangun kapasitas sumber daya penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah
d. mendorong pembentukan CSIRT (*Computer Security Incident Response Team*) pada sektor pemerintah

3.2. Konstituen

Konstituen Gov-CSIRT Indonesia meliputi Pemerintah Pusat, Pemerintah Daerah wilayah I, dan II yaitu :

a. Pemerintah Pusat adalah Presiden Republik Indonesia yang memegang kekuasaan pemerintahan negara Republik Indonesia yang dibantu oleh Wakil Presiden dan Menteri sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
b. Pemerintah Daerah Wilayah I adalah Pemerintah Daerah Provinsi yang meliputi wilayah Provinsi Aceh, Sumatera Utara, Riau, Sumatera Barat, Kepulauan Riau, Jambi, Sumatera Selatan, Bangka Belitung, Bengkulu, Lampung, Daerah Khusus Ibu Kota Jakarta, Jawa Barat, Banten, Jawa Tengah, Daerah Istimewa Yogyakarta, Jawa Timur, dan Bali
c. Pemerintah Daerah Wilayah II adalah Pemerintah Daerah Provinsi yang meliputi wilayah Provinsi Kalimantan Barat, Kalimantan Tengah, Kalimantan Selatan, Kalimantan Timur, Kalimantan Utara, Sulawesi Utara, Gorontalo, Sulawesi Tenggara, Sulawesi Tengah, Sulawesi Selatan, Sulawesi Barat, Nusa Tenggara Timur, Nusa Tenggara Barat, Papua Barat, Papua, Maluku, dan Maluku Utara

3.3. Sponsorship dan/atau Afiliasi

Gov-CSIRT Indonesia merupakan bagian dari BSSN sehingga seluruh pembiayaan bersumber dari APBN.

3.4. Otoritas

Berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 tentang BSSN sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017, Gov-CSIRT Indonesia memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada sektor pemerintah.

Gov-CSIRT Indonesia melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya.

4.1. Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

Gov-CSIRT Indonesia memiliki otoritas untuk menangani berbagai insiden keamanan siber yang terjadi atau mengancam konstituen kami (dapat dilihat pada Subbab 3.2).

Dukungan yang diberikan oleh Gov-CSIRT Indonesia kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Gov-CSIRT Indonesia akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber.

Seluruh informasi yang diterima oleh Gov-CSIRT Indonesia akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa Gov-CSIRT Indonesia dapat menggunakan alamat *e-mail* tanpa enkripsi data (*e-mail* konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada *e-mail*.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke bantuan70[at]bssn.go.id dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. *Disclaimer*

Tidak ada

5.1. Respon Insiden

Gov-CSIRT Indonesia akan membantu konstituen untuk melakukan penanggulangan dan pemulihan insiden keamanan siber dengan aspek-aspek manajemen insiden keamanan siber berikut :

5.1.1. Triase Insiden (*Incident Triage*)

a. Memastikan kebenaran insiden dan pelapor
b. Menilai dampak dan prioritas insiden

5.1.2. Koordinasi Insiden

a. Mengkoordinasikan insiden dengan konstituen
b. Menentukan kemungkinan penyebab insiden
c. Memberikan rekomendasi penanggulangan berdasarkan panduan/SOP yang dimiliki Gov-CSIRT Indonesia kepada konstituen
d. Mengkoordinasikan insiden dengan CSIRT atau pihak lain yang terkait

5.1.3. Resolusi Insiden

a. Melakukan investigasi dan analisis dampak insiden
b. Memberikan rekomendasi teknis untuk pemulihan pasca insiden
c. Memberikan rekomendasi teknis untuk memperbaiki kelemahan sistem

5.2. Aktivitas Proaktif

Gov-CSIRT Indonesia secara aktif membangun kesiapan instansi pemerintah dalam melakukan penanggulangan dan pemulihan insiden keamanan siber melalui kegiatan :

a. *Cyber Security Drill Test*
b. *Workshop* atau Bimbingan Teknis
c. Asistensi Pembentukan CSIRT organisasi

UNIT KERJA MENANGANI CSIRT

Pelayanan CSIRT berada di unit kerja yang menyelenggarakan fungsi TIK dan Keamanan informasi sehingga CSIRT dilaksanakan oleh Organisasi Perangkat Daerah yang memiliki kewenangan di bidang tersebut.

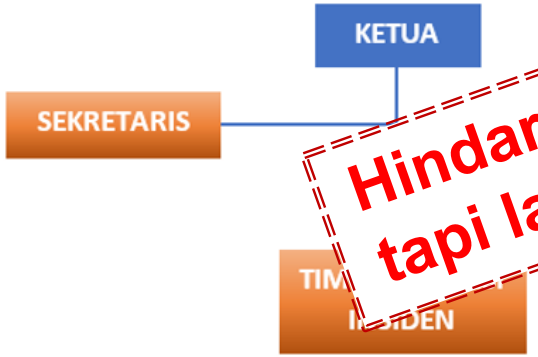
- Kementerian /Lembaga (K/L) : Pusdatik /Pusdatin /Pusdasi
- Pemerintah Daerah (Pemda) : Dinas Kominfo

BADAN SIBER & SANDI NEGARA

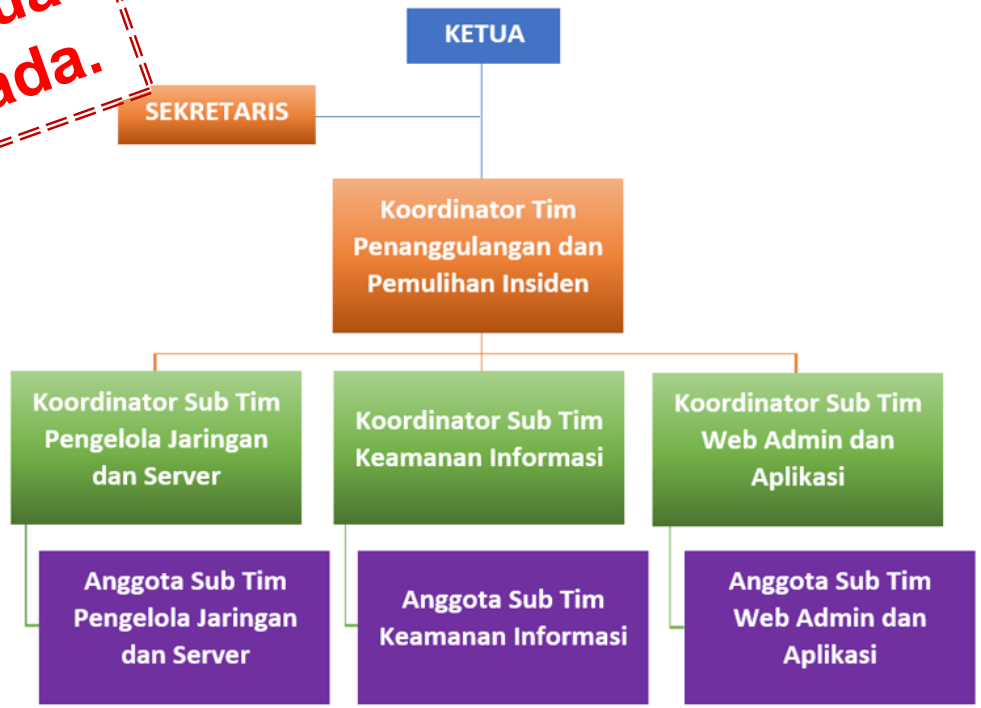
MENYUSUN TIM CSIRT

Tim CSIRT dibentuk berdasarkan layanan yang diberikan kepada konstituen dan keahlian staf yang dimiliki.

CONTOH

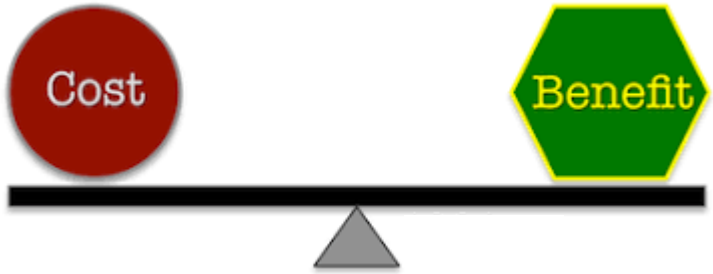
LAYANAN	TIM INTERNAL	STRUKTUR CSIRT
KOORDINASI INSIDEN	TANPA TIM INTERNAL	

Hindari struktur dibuat tapi layanan tidak ada.

LAYANAN	TIM INTERNAL	STRUKTUR CSIRT
RESPON INSIDEN	MEMILIKI TIM INTERNAL	

BIAYA OPERASIONAL

Kebutuhan biaya operasional CSIRT, berdasarkan Layanan yang diberikan serta jumlah staf CSIRT /keahliannya. Sebaiknya manfaat yang diberikan sebanding dengan biaya yang dikeluarkan.

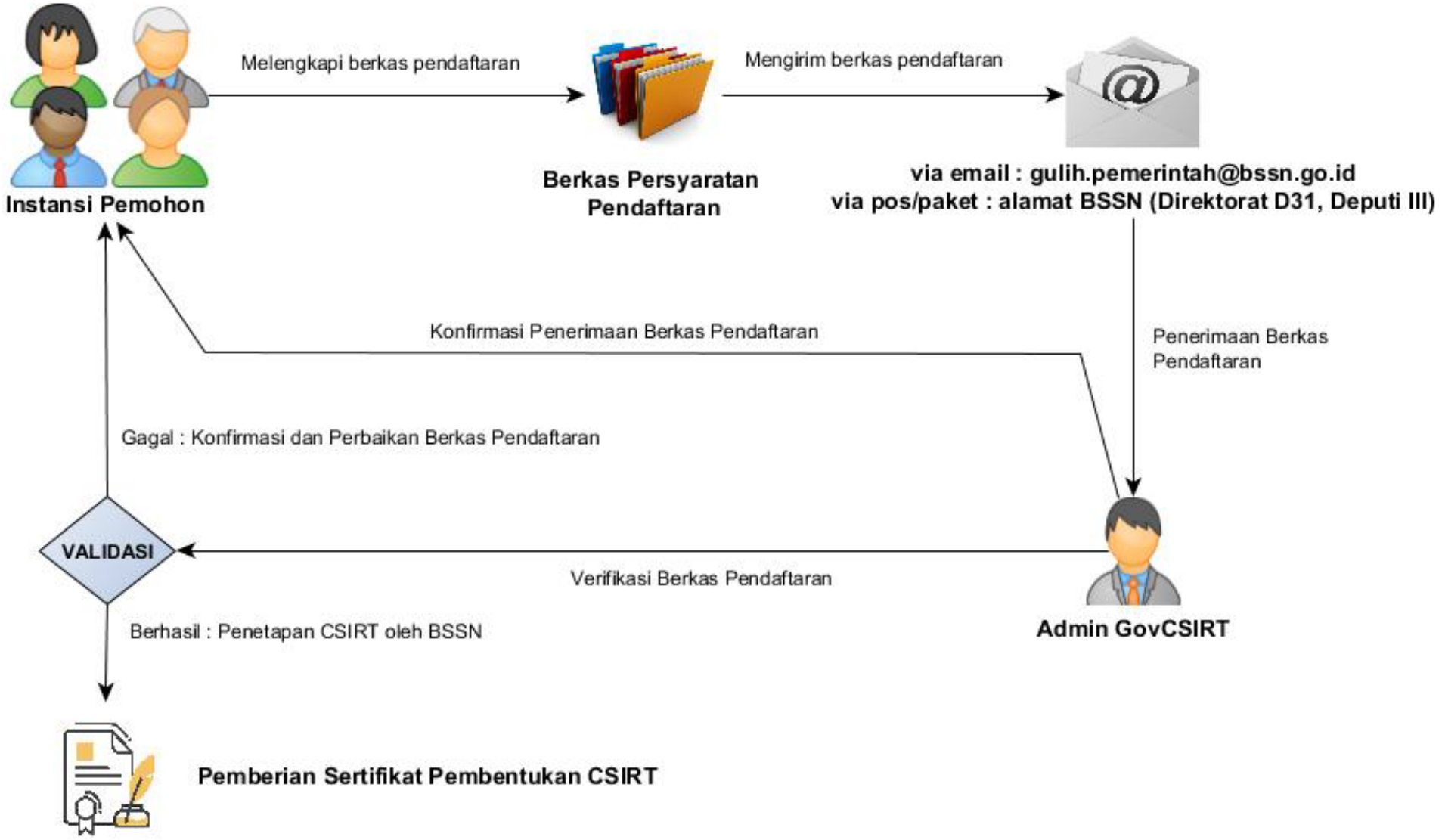


- Pengelolaan web CSIRT
- Tim piket
- Biaya respon
- Seminar /workshop /pelatihan

KEBUTUHAN PERANGKAT

LAYANAN	TIM INTERNAL	PERANGKAT
KOORDINASI INSIDEN	TANPA TIM INTERNAL	❑ Publikasi web CSIRT Digabungkan dengan website utama ❑ Pembuatan web K/L atau Pemda CSIRT Server, Aplikasi Web, Firewall, AntiVirus
RESPON INSIDEN	MEMILIKI TIM INTERNAL	❑ Publikasi web CSIRT Digabungkan dengan website utama ❑ Pembuatan web K/L atau Pemda CSIRT Server, Aplikasi Web, Firewall, AntiVirus ❑ Log Analyzer, Vulnerability Scanner, Forensic, Analisa Malware

MEKANISME PENDAFTARAN CSIRT



TAHAPAN pendaftaran csirt

PENGAJUAN PENDAFTARAN

1

PENGIRIMAN BERKAS PENDAFTARAN

2

VALIDASI BERKAS PENDAFTARAN

3

PEMBERIAN SERTIFIKAT PEMBENTUKAN CSIRT

4

BADAN SIBER & SANDI NEGARA

BADAN SIBER &
SANDI NEGARA

TERIMA KASIH