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. Informasi Data/Kontak

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 Selatan
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-mail*)

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+vW7j5K3AIEHVYFLYnU8F0FqBpcyFFlAWhqRgp6Jscsn9w0Ty
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/l3x482/7yJS6oEIhqY17nskNFjmBqM6fwTFdQybarqs1AgxN3ne26MWs
VcmhSLsOaiN7tEnD0jPIRgqCZ4SnXeqthbuIoCb6cMI4Mae1gRRM4pb1ec4OyriW
infNAa+zWolZNuQG0cz/xuVme34Imv3Nv9WutCuyjGR3RenixIg68Sww7tV4x3gw
bkqu/3HReG9t39maeDafw6w0//oHyAqPA8vk36sK9Pt0zjro/q8s8W3NzsHnh/Ca
HX40WsX7oZPGBm0ILdHxwCXhhXmBY/aYBsSIC4AvYLrHRTHFCWxk6B6pL8rte06b
xyzICVQmQJLfn/QF9OhttIpYTY02yppGRRs9Tvyf+xTfZyIMoKeDjJmymZ1D421B
BguRR+zaxdrQwza1B3RIQ+8VKG/Mjf/zmnRAxSssXLm4LJ/KtpFWhI1lUDMhaMc8
fFOxH3Oj+N+tAPvM34LN1EJrDR/r6AggwBciM5ak1gtijlJS85NLFWHbFhQwHdZM
3kiTYNgYJ2uvfq7enswzMk/jy2bjd17UVTzfxpg3gz0iZ52hBnHl8DEtw4l5KQgS
ys4Nmen51ZylyT+NfD73vk3nS41cI36d4YV97FlQ7rbaitNVFFBKV5fVSfkFrwKW
akU0T8oeCOiNuwLQWXdg3447BLyhNObQWL3YoKq5Ag0EW17HhAEQALwqDRRG5byw
MDLVQTTWdqeK5cezTKw5Ebj50tk0VSTaG3hDfwkwyPJjzTkuwPUEQb+6mEtOqQ2P
x9jlQylumI0Uy3NBd5wkaS9ZxEa9HU70VXeDlvAx+0eJeVNMCUcdgU28/nCnzAIr

3+5lseTg4MRrSo9xfgqYFd+QE5wmYGRO7/gXhvMf9vrVr8lcIvWWxYKUGl0bYoct
5ZSepTZ2mDJoJoOeuoTMW0WOfbGHzs1jS950PqXri+n9LzupYc2FF3NEBRw1NuLY
MnwwDkqbGeLSnFEaOXce8BD9Ppnh1CK0dMwTWBCUlAUJXRNWRMN5prREs8gVRkJ0
GuRaMmji+lJHg5HfuXV3zKWJ3UBnCM1MpIpvFReMH2OPHWzeObAXcpg6OsPCk+99
MLjmkC/C2cZtHf48JJCRMtrTUN0165DJFXoJcCinaNRUx+YnHVTC5Wuu4+DVaCzY
5WbNc6LaQkA1PMK9oqBXFDtERXirbacw4kOpvoC+J0B6xnYDrAOQ8cAc9pSO7QSf
Y0NZYhDoJz6o5++TSt6P8Ol/LdsVFIK0TLhf1qiqMhuibCQi6Fom7r6D5wtuZ+22
Mn2Jw8nuMYvo7ze3p5jwoErCpPswh6AqSia8kTgMUoDNPJwuoC7m0dzWvQ99reNr
K9QdhjC3LtclPQolqibVz/Hfm3trciGlABEBAAGJAjwEGAEIACYWIQQaNdrv5ju+
k8MUMnLOXSEZc4Ar1gUCW17HhAIbDAUJCWYBgAAKCRDOXSEZc4Ar1jzKEACI7rht
7nF1cYEZpbwU3u8MTZXSCxu/kgmxYmJlnQhRhahwtWf5N/xn0lJtMGoic5wbpAvu
JqE/5OOTyd3dUx5eOtBjaEFf5Zw1Ar96K9x764YtJIyiq2WYuMK2EEYX8uoqpGCu
9iGqnis1EWOca5cSzjo60McN+UoMSTItja8XgLOAVkIxcz9CepRucBf/yugc6ENT
eUcA6Dv84tO4f0E5aKuXxk7ESMk/Whukz2PCsSaqs5K+1yCAZvU2aio4XYr2GJr9
VpI++A57r7lJqrhdIUJjuJmLGdV1HOTl3ITWkXi4XhNbsgeAjZ9iU3wjl1kSwf3P
aunf2wLww+j9sTuIalZ6UWpnLCRbsA8IkVtFFczuM4NrBktFKx5y1QmdfTHgsmCS
8McEOEOZyGLngRWUwuhrKQI7okrxXhbQGMlNdSQ1luPw0Bx7aYsUWnEFqMOApLAB
2Zm7CqYfrwsNGp6sWAwimO+05AOvr7jcqeBfwYyfDImO0Rf75YjPU6yJ+4NyEUWE
JubnHIYk47fV4T6O7BjvdgHIYHe51qDKo6xxmt32Wcn05fzGxTaPclgBC3krrwNB
vkPTTMDlkJ6fEBe5q476Xs+7RPRmlr4FE5tu7/GoVGKJCKIvXJWCZrYawhACjE8h
WGksMO/XgZgXAA1/KIljfJUJ0rjPMjgktq23Zg==
=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

2.9. Anggota Tim

Ketua Gov-CSIRT Indonesia adalah Direktur Penanggulangan dan Pemulihan Pemerintah, Deputi Bidang Penanggulangan dan Pemulihan, BSSN. Yang termasuk anggota tim adalah seluruh staf BSSN di sektor pemerintah.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak Gov-CSIRT Indonesia

Metode yang disarankan untuk menghubungi Gov-CSIRT Indonesia adalah melalui *e-mail* pada alamat bantuan70[at]bssn.go.id atau melalui nomor telepon (021) 78833610 ke Pusopskamsinas yang siaga selama 24/7.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi Gov-CSIRT Indonesia adalah terwujudnya ketahanan siber pada sektor pemerintah yang andal dan profesional.

3.2. Misi

Misi dari Gov-CSIRT Indonesia, yaitu :

a. mengkoordinasikan dan mengolaborasikan layanan keamanan siber pada sektor pemerintah;

b. membangun kapasitas sumber daya keamanan siber pada sektor pemerintah.

3.3. Konstituen

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

a. Pemerintah Pusat adalah Lembaga Tinggi Negara, Kementerian, Lembaga Pemerintah Non Kementerian, dan Lembaga Non Struktural yang memiliki kedudukan strategis;
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.

3.4. Sponsorship dan/atau Afiliasi

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

3.5. 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. Kebijakan – Kebijakan

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

Gov-CSIRT Indonesia memiliki otoritas untuk menangani insiden yaitu :

a. *Web Defacement*;
b. DDOS;
c. *Malware*;
d. *Phising*;

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*.

5. Layanan

5.1. Layanan Reaktif

Layanan reaktif dari Gov-CSIRT Indonesia merupakan layanan utama dan bersifat prioritas yaitu :

5.1.1. Layanan pemberian peringatan terkait dengan laporan insiden siber

Layanan ini dilaksanakan oleh Pusat Operasi Keamanan Siber Nasional BSSN berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh Gov-CSIRT Indonesia.

5.1.2. Layanan penanggulangan dan pemulihan Insiden

Layanan ini diberikan oleh Direktorat Penanggulangan dan Pemulihan Pemerintah BSSN berupa koordinasi, analisis, rekomendasi teknis, dan bantuan *on-site* dalam rangka penanggulangan dan pemulihan insiden siber. Gov-CSIRT Indonesia memberikan informasi statistik terkait layanan ini.

5.1.3. Layanan penanganan kerawanan

Layanan ini diberikan oleh Direktorat Proteksi Pemerintah BSSN berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*), Gov-CSIRT Indonesia memberikan informasi statistik terkait layanan ini. Namun, layanan ini hanya berlaku apabila syarat-syarat berikut terpenuhi :

a. Pelapor atas kerawanan adalah pemilik sistem elektronik. Jika pelapor adalah bukan pemilik sistem, maka laporan kerawanannya tidak dapat ditangani;
b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *Vulnerability Assessment.*

5.1.4. Layanan penanganan artifak

Layanan ini diberikan oleh Direktorat Penanggulangan dan Pemulihan Pemerintah BSSN dan Direktorat Pengendalian Informasi, Investigasi, dan Forensik Digital BSSN berupa penanganan artifak dalam rangka pemulihan

sistem elektronik terdampak ataupun dukungan investigasi. Gov-CSIRT Indonesia memberikan informasi statistik terkait layanan ini.

5.2. Layanan Proaktif

Gov-CSIRT Indonesia secara aktif membangun kapasitas sumber daya keamanan siber melalui kegiatan :

5.2.1. Pemberitahuan hasil pengamatan terkait dengan ancaman baru

Layanan ini diberikan oleh Direktorat Deteksi Ancaman BSSN berupa hasil dari sistem deteksi dini Honeynet BSSN. Gov-CSIRT Indonesia memberikan informasi statistik terkait layanan ini.

5.2.2. Layanan *security assessment*

Layanan ini diberikan oleh Direktorat Identifikasi Kerentanan dan Penilaian Risiko Pemerintah BSSN berupa identikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan. Gov-CSIRT Indonesia memberikan informasi statistik terkait layanan ini.

5.2.3. Layanan *security audit*

Layanan ini diberikan oleh Direktorat Proteksi Pemerintah BSSN berupa penilaian keamanan informasi. Gov-CSIRT Indonesia memberikan informasi statistik terkait layanan ini.

5.3. Layanan Manajemen Kualitas Keamanan

Gov-CSIRT Indonesia meningkatkan kualitas keamanan melalui kegiatan :

5.3.1. Konsultasi terkait kesiapan penanggulangan dan pemulihan Insiden

Layanan ini diberikan Gov-CSIRT Indonesia berupa pemberian rekomendasi teknis berdasarkan hasil analisis terkait penanggulangan dan pemulihan insiden.

5.3.2. Pembangunan kesadaran dan kepedulian terhadap keamanan siber

Dalam layanan ini Gov-CSIRT Indonesia mendokumentasikan dan mempublikasikan berbagai kegiatan yang dilakukan oleh unit kerja BSSN dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber yaitu :

a. Direktorat Identifikasi Kerentanan dan Penilaian Risiko Pemerintah;
b. Direktorat Deteksi Ancaman;
c. Direktorat Proteksi Pemerintah;
d. Direktorat Penanggulangan dan Pemulihan Pemerintah BSSN;
e. Direktorat Pengendalian Informasi, Investigasi, dan Forensik Digital .

5.3.3. Pembinaan terkait kesiapan penanggulangan dan pemulihan insiden

Gov-CSIRT Indonesia menyiapkan program pembinaan dalam rangka pendukung penanggulangan dan pemulihan insiden.

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*

Terkait penanganan jenis *malware* tergantung dari ketersediaan *tools* yang dimiliki.