RFC 2350 LIPI – CSIRT

1. Informasi Mengenai Dokumen

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

1.1 Tanggal UpdateTerakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 11 Februari 2021.

1.2 Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3 Lokasi dimana Dokumen ini bisa didapat

-

1.4 Keaslian Dokumen

-

1.5 Identifikasi Dokumen

Judul	:	RFC 2350 LIPI-CSIRT;
Versi	:	1.1;
Tanggal Publikasi	:	11 Februari 2021;
Kadaluawarsa	:	Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Kontak

2.1 Nama CSIRT

Lembaga Ilmu Pengetahuan Indonesia – CSIRT

Disingkat : LIPI – CSIRT

2.2 Alamat Kantor

Pusat Data dan Dokumentasi Ilmiah, LIPI
Jl. Jend. Gatot Subroto No. 10, Jakarta 12710
Jakarata – Indonesia

2.3 Zona Waktu

Jakarta (GMT + 07:00)

2.4 Nomor Telepon

(Tidak ada)

2.5 Nomor Fax

(Tidak ada)

2.6 Telekomunikasi Lain

(Tidak ada)

2.7 Alamat Surat Elekktronik (E-mail)

csirt@mail.lipi.go.id

2.8 Informasi kunci publik dan enkripsi

(Tidak ada)

2.9 Anggota Tim

Ketua LIPI-CSIRT adalah Koordinator Pelaksana Fungsi Pengelolaan Infrastruktur dan Dukungan IT, Pusat Data dan Dokumentasi Ilmiah, LIPI. Yang termasuk anggota tim adalah Koordinator, Subkoordinator IT Kawasan dan Pelaksana Fungsi Pengelolaan Infrastruktur dan Dukungan IT.

2.10 Informasi/Data lainnya

(Tidak ada)

2.11 Catatan-catatan pada Kontak LIPI-CSIRT

Metode yang disarankan untuk menghubungi LIPI-CSIRT adalah melalui e-mail pada alamat csirt@mail.lipi.go.id.

3. Mengenai LIPI-CSIRT

3.1 Misi

Tujuan dari LIPI-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 LIPI-CSIRT Indonesia meliputi seluruh satuan kerja di lingkungan LIPI

3.3 Sponsorship dan/atau Afiliasi

LIPI-CSIRT merupakan bagian dari LIPIsehingga seluruh pembiayaan bersumber dari anggaran LIPI.

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. Kebijakan – Kebijakan

4.1 Jenis-jenis Insiden dan Tingkat/Level Dukungan

LIPI-CSIRT memiliki otoritas untuk menangani berbagai insiden keamanan siber yang terjadi atau mengancam konstituen kami (dapat dilihat pada Subbab 3.2). Dukungan yang diberikan oleh LIPI-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data LIPI-CSIRT akan melakukan kerjasama dan berbagi informasi denganCSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh LIPI-CSIRT akan dirahasiakan.

4.2 Komunikasi dan Autentikasi

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

5. Layanan

5.1 Respon Insiden

Untuk komunikasi biasa LIPI-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.

5.1.1 Triase Insiden (Incident Triage)

a. Memastikan kebenaran insiden dan pelapor

b. Menilai dampak dan prioritas insiden

5.1.2 Koordinasi Insiden

a. Mengkoordinasi insiden dengan konstituen

b. Menentukan kemungkinan penyebab insiden

c. Memberikan rekomendasi penanggulangan berdasarkan panduan/SOP yang dimiliki LIPI-CSIRT 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 LIPI-CISRT menyajikan data statistic mengenai insiden yang terjadi pada sektor pemerintah sebagai untuk sentra informasi keamanan siber pada sektor pemerintah

5.2 Aktivitas Proaktif

LIPI-CSIRT secara aktif membangun kesiapan LIPI dalam melakukan penanggulangan dan pemilihan insiden keamanann siber melalui kegiatan:

a. Cyber Security Drill Test

b. Workshop atau Bimbingan Teknis

c. Asistensi Pembentukan CSIRT organisasi

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirim ke csirt@mail.lipi.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)