RFC 2350 SETNEG - CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 23 November 2020.

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://setneg.go.id/setneg-csirt (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen ini ditandatangani digital menggunakan sertifikat digital BSSN oleh Sekretaris Kementerian Sekretariat Negara.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 Setneg-CSIRT;
Versi : 1.1;
Tanggal Publikasi : 23 November 2020
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Kementerian Sekretariat Negara – *Computer Security Incident Response Team* (CSIRT), disingkat: Setneg-CSIRT

2.2. Alamat

Kementerian Sekretariat Negara
Jl. Veteran No. 17 – 18
Jakarta Pusat 10110
Indonesia

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

Telepon (021) 3458595

2.5. Nomor Fax

Tidak ada

2.6. Telekomunikasi Lain

Tidak ada

2.7. Alamat Surat Elektronik (*E-mail*)

csirt@setneg.go.id

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

Tidak ada

2.9. Anggota Tim

Ketua Setneg-CISRT adalah Sekretaris Kementerian Sekretariat Negara, Kementerian Sekretariat Negara. Yang termasuk anggota tim adalah seluruh perwakilan unit pengelola TI pada Biro Informasi dan Teknologi di Kementerian Sekretariat Negara.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak Setneg-CSIRT

Metode yang disarankan untuk menghubungi Setneg-CSIRT adalah melalui e-mail pada alamat csirt@setneg.go.id atau melalui nomor telepon (021) 3458595.

3. Mengenai Setneg-CSIRT

3.1. Visi

Visi Setneg-CSIRT adalah terwujudnya ketahanan siber di lingkungan Kementerian Sekretariat Negara yang andal dan profesional.

3.2. Misi

Misi dari Setneg-CSIRT, yaitu :

a. Mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi;

b. membangun kesadaran keamanan siber pada sumber daya Manusia di lingkungan Kementrian Sekretariat Negara.
c. Melakukan evaluasi berkala terhadap Kehandalan Keamanan teknologi informasi di lingkungan Kementrian Sekretariat Negara.

3.3. Konstituen

Mencakup Semua Satuan Kerja dalam Kementerian Sekretariat Negara kecuali Satuan Kerja Sekretariat Presiden dan Sekretariat Wakil Presiden

3.4. Sponsorship dan/atau Afiliasi

Biro Informasi dan Teknologi

3.5. Otoritas

Setneg-CSIRT memiliki kewenangan secara administratif dengan konstituenya dalam penangan insiden.

4. Kebijakan – Kebijakan

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

Setneg-CSIRT Indonesia memiliki otoritas untuk menangani insiden yaitu :
a. *Web Defacement*;
b. DDOS;
c. *Malware*;
d. *Phising*;

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Setneg-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber.
Seluruh informasi yang diterima oleh Setneg-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa Setneg-CSIRT Indonesia dapat menggunakan alamat *e-mail* dan telepon.

5. Layanan

5.1. Layanan Reaktif

5.1.1. Pencegahan terhadap Inciden

Layanan ini dilaksanakan oleh Biro Informasi dan Teknologi berupa layanan teknis untuk *hardening* pada perangkat *end user* maupun pada infrastruktur jaringan guna mencegah adanya *security incident.*

5.1.2. Penanganan dan penanggulangan Insiden

Layanan ini merupakan layanan teknis berupa penanganan insiden yang terjadi pada Konstituen Setneg-CSIR. Layanan ini bertujuan untuk menangani sebuah insiden dan melakukan tindakan guna mencegah sebuah insiden tidak terulang kembali.

5.1.3. Layanan penanganan kerawanan

Layanan ini berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*) dalam konstituen Setneg-CSIRT.

5.2. Layanan Proaktif

5.2.1. Sosialisasi *Security Awareness*

Layanan ini diberikan oleh Biro Informasi dan Teknologi berupa sosialisasi kepada pegawai di lingkungan Kementerian Sekretariat Negara yang bertujuan untuk meningkatkan kesadaran dan kepedulian para pegawai tentang keamanan Teknologi Informasi.

5.2.2. Layanan *Helpesk*

Layanan ini merupakan portal antara Biro Informasi dan Teknologi dengan Konstituen Setneg–CSIRT. Helpdesk ini digunakan untuk mempermudah koordinasi dan juga dilakukan untuk penanganan *security incident.*

5.2.3. Layanan *Security Reporting*

Layanan ini berupa analisa dan statistik *report* bulanan yang dihasilkan dari perangkat-perangkat security. Hasil dari analisa tersebut dapat dijadikan sebagai dasar untuk membuat sosialisasi media elektonik berupa animasi atau poster yang dibagikan kepada pegawai Kementrian Sekretariat Negara.

5.3. Layanan Manajemen Kualitas Keamanan

5.3.1. Analisis Risiko

Layanan ini berupa Analisa risiko yang dihasilkan dari perangkat-perangkat security. Hasil dari Analisa tersebut dapat dijadikan sebagai dasar untuk peningkatan layanan dalam penanganan *security incident*.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@setneg.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.