RFC 2350 SemarangKota-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 28 Desember 2021.

1.2. Daftar Distribusi untuk Pemberitahuan

Dinas, Badan, dan OPD konstituen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.semarangkota.go.id/rfc2350-id.pdf (versi Bahasa Indonesia)
https://csirt.semarangkota.go.id/rfc2350-en.pdf (versi Bahasa Inggris)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik SemarangKota-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 SemarangKota-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 28 Desember 2021;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team (CSIRT) Pemerintah Kota Semarang
Disingkat : SemarangKota-CSIRT.

2.2. Alamat

Dinas Komunikasi Informatika Statistik dan Persandian Kota Semarang
Jl. Pemuda no. 148, Sekayu, Semarang Tengah, Semarang
Indonesia

2.3. Zona Waktu

Semarang (GMT+07:00)

2.4. Nomor Telepon

(024)3549446

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

-

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

csirt@semarangkota.go.id

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

Bits : 4096
ID : BA7A4BC74A79B712
Key Fingerprint : 2dae999d6b194795d69a7458ba7a4bc74a79b712

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGIAyFkBEADGU6yvZduRhtxPGAKNoSTFknwrga5X6f0xblKI1zZjiHknlcDS
RC0T9T/FCo4eQxCDn6ho2h+JqFcoM8+n/dGMptih1sYkGOnB9GOH8rMA905EFG6L
4oKuiPP/yFS+GZTTiKwvTe1C5BqG8HtQm7/Gp/UydAXVMJbGOSjibbfB/tPGhSpJ
FyG+GDGkmu5TbcGuwkWEv2T4XUITA7WjZZA8Rmj3GoPgHrlQYPBw7dmuK0BHTrFJ
eC0Vc6naudVcCqb9Ju0XBS+Hog0D6RM80mjQn6bWGr1eWq21x8wQenNfMbsCPN7m
e4aiaHEAHzu9/EXoc1ZHCBpeZFkPDC8whtuKZ0ioD7KqAeaJXFRqi46woTDvTeKA
EK9bki6Fkv00aVXYrgmP3LCwiSIBaAx7xexIwL5gsmpAD5dAJYkN3MlernlJ8F1e
5xaIK027/T2WOykWlSqG6GYsWL9BVIK8/Jc8iKfcIpavKSUuPB3v1KkVtM16AFqE
irwx/pYK3uapDXZNhZmFsxl/zZK8GfdLC+u+Pr7DeiqXFkegDgW+m7i3R6mbY+GG
rEujZ5biKZvsMlKyGFUlo1TRcloTVKt8FwWl9NLutVNQf2jDESnS+pUvcvE1FiKV
t0LyTPEWx4SRxZRRTIf986Qp7IecGUr6lbZqFerdB6VNTQr5LsBKDTKMJwARAQAB
tC1TZW1hcmFuZ0tvdGEtQ1NJUlQgPGNzaXJ0QHNlbWFyYW5na290YS5nby5pZD6J
AlgEEwEIAEIWIQQtrpmdaxlHldaadFi6ekvHSnm3EgUCYgDIWQIbAwUJA8JF9wUL
CQgHAgMiAgEGFQoJCAsCBBYCAwECHgcCF4AACgkQunpLx0p5txKzIhAAmbDADjAN
m2VQiz3/WfNAOoFKkTja417Nyy+cRHEkOJBa4ZgGpbm7yoEaddK9DkazVwzXXPVh
N+FFeZ63RrK+8dA1QQgYFdt04IMmNnUkUp7JNF2a8XyDLvNmyfQrG/62QgS3FIFB
m3L6Ujf0ydmWfNKwYTGvxuNNArnYhEqB5COrPMeMheGJikUJzy0hxgivZssfCthS
pjkjGcG5MhKQoMQehoXrrXc/9u58xzWjXA7Zdz6eyrH8jYaM+KkfAX2VAOht6S6e
O5j6blLSH9xY+qN22C3AnD41BuboumBcTRxAJsc86O1C0iFBOf4uSHW4lTwPr4Pk
d4hL8FVBn6uoMHgUfZNk0MpqdsLgx2eMUqX/A1rwDqWZpZp23hJwRxL0JQBODHrx
/1U0+3pn4GHexny9gwwDS5GOyJob5y5yDOm576cwlMXcgue5F7eHi9lCjPOPGtLR
lVM/LZ8YckZbCuFg9xSBS7Bjnvwrdia5GqW8I7b1vzYAEL8QIODMZhOlW8upwYOi
zlRWumRr3T+6GutlxKqtMtvBKJTpj+ceLR57YtMGMtafixlJjpZ0BuoHR5ipmACr
w6FpM5eyFVIonGYVDpc17fLOjHilDKdgO6otOrBDZ8sfeBc5wCHRJAj0FKT0keyn
auOj9UPkZm0dyiQhqdMWxIJyBjQKMDxD2XK5Ag0EYgDIWQEQANGlz6GBf/jKCjvj
KUMPrc/jxbPtaI7NbDsEZRg7nJkfZlft/vhv60JMA7HANK2ntIJaOTVAw06faZK5
z2vRKZhi8jh2l2DSFAfrXh9Rl+U+kONZh4hVEHsuWSovs+pApktYEtsdR0d4ZK0h
IehT4LilygTCMPzGgw5LK/WS0J6ZJfcahQKrkY7gP6kqmT2KDAfyQKGtHzlUDSPJ
zvh+6KmKH+GxwLPvl3yCy5ShdptXMYpNC1639xCrNKgtOXbm7KqssX/sWZ7qWb7K
vA+80jOVuRlQlgArRfThQeIsDGPRRftDz9L0ducd4fZCVBm8nyCsjb11yHUs9LgS
ckFfs7OJ7jIzawsTogkfTEVnfGYqc66p8YZWmgWv0nFtZwHA93ACTR/g22+Nopzt
WFk+EfFcjHT6Dp9nna18GPISs/EKiMrEghNipc7YOS4PYHgEBWLAZZwnCYqVSEJ1
/YNmTjJMND0JsfWYIRXT2CHaGGtNWKD5tree9k9wA8xwWw1cOmP2af97VQWoAmoz
MUUMjBxkBq/X9I7nVJR011hAC3zgPh6vscSnIGF++ULXk+T6+wr1U75ejLCQQIh8
ZORtzP+fLKJw2IoLWamnm2d74gE0zVQ1zMn5vi3sS1EguZW/2718xZ+HLxqQXvRG
vT+M756B/kma3sJSDUtmZzKWTPaXABEBAAGJAjwEGAEIACYWIQQtrpmdaxlHldaa
dFi6ekvHSnm3EgUCYgDIWQIbDAUJA8JF9wAKCRC6ekvHSnm3EgdaD/4pXPFL4A4V
41ZL9ckVYe+FbXph+4rGdfQzlKYW5s7QXsYA/fQqqATLGSM683JmxmROkiP8waug
yBwg/MwtimHpKBoJuw254CA7meLP/yxGz3wlF/ZL2mS8XBPPYxZo6UpTZfhNezQ2
zKETCdcxtfX7Sl6Brp1uu/JEZ4xc+fCVrORnwCmU645HIB0v+cuKppLqFoVm3/2J
eWFUlPksazjC4kCH2ab0bLawioZOf8Ek1L4db3tpsnTneNjR+H7+oESPObIU4JJD
AQZ26WhzWtq2ipNzPMYc0AOD1R44O72Hjwt1MVRgkEmQDYXzFpCvqUpOswLEYeWe
jvL2NmRNDkhKSqtUQS0XWLak+kBQVhLi08VFKAbAVQppE3hAZ58PHk4xpr3oDI38
BnqxPKTpY3Psjv2GYvAyYDxQZtdXTYTVMYiQ5RX0GCOJJUlLZdDooc48ylEdrhVv
kOagPzMopP3wXMbCX6dSLjMYoXm7aVGEYb88bfTHYTWlnfUXauhy2KOgSc9Cr5tS
wId8Zc+sNa/jPoYXmfcVJDXYpxyDfuZfMGvXdq9tJ0PrLWtsDHDx9j/sa/9Yxk13
WXr+Q3qmDJQOIEO2mlgsTbWp9Jj53r3Jm9n1yPTf1g4tYUkClBDoTnmN2XW/9tse
Qb6Uawa9+shttCtl6DLHZjiD36gHMZ5ZVA==
=9cXx
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.semarangkota.go.id/SemarangKota-CSIRT_0x4A79B712_public.asc

2.9. Anggota Tim

Penanggungjawab SemarangKota-CSIRT adalah Sekretaris Daerah Kota Semarang, Ketua SemarangKota-CSIRT adalah Kepala Dinas Komunikasi Informatika Statistik dan Persandian (Diskominfo) Kota Semarang, Sekretaris SemarangKota-CSIRT adalah Sekretaris Diskominfo Kota Semarang, Koordinator I Tim Resolusi Insiden adalah Kepala Bidang Layanan E-Government pada Diskominfo Kota Semarang, Koordinator II Tim Resolusi Insiden adalah Kepala Bidang Pengelolaan Infrastruktur pada Diskominfo Kota Semarang, Koordinator I Tim Pemulihan Insiden adalah Kepala Seksi Layanan Infrastruktur, Internet dan Intranet pada Diskominfo Kota Semarang, Koordinator II Tim Pemulihan Insiden adalah Kepala Seksi Keamanan Informasi dan Persandian pada Diskominfo Kota Semarang. Yang termasuk anggota tim adalah Kepala Seksi Pengelolaan TIK, Kepala Seksi Pengembangan dan Pengelolaan Aplikasi, Kepala Seksi Layanan Manajemen Data, Pengelola Teknologi Informasi dan Komunikasi pada seluruh Perangkat Daerah di Lingkungan Pemerintah Kota Semarang, Pakar/Tenaga Ahli Pengembangan Aplikasi, Pakar/Tenaga Ahli Jaringan, Pakar/Tenaga Ahli Data Center, dan Pakar/Tenaga Ahli Keamanan Aplikasi.

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak SemarangKota-CSIRT

Metode yang disarankan untuk menghubungi SemarangKota-CSIRT adalah melalui *e-mail* pada alamat csirt[at]semarangkota[dot]go[dot]id atau melalui nomor telepon (+62) 24 3549446 ke Tim SemarangKota-CSIRT siaga selama pukul 07.30-15.30 hari Senin-Kamis dan jam 07.30-11.30 hari Jumat.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi SemarangKota-CSIRT adalah terwujudnya ketahanan siber pada lingkungan Pemerintah Kota Semarang yang andal dan professional demi terwujudnya Sistem Pemerintahan Berbasis Elektronik yang terpadu dan menyeluruh untuk mencapai birokrasi dan pelayanan publik yang hebat.

3.2. Misi

Misi dari SemarangKota-CSIRT, yaitu :

a. Mengkoordinasikan dan mengolaborasikan layanan keamanan siber pada lingkungan Pemerintah Kota Semarang dalam hubungannya dengan tata kelola sistem pemerintahan berbasis elektronik dan pelayanan publik yang terpadu, menyeluruh dan menjangkau masyarakat luas;
b. Membangun kapasitas sumber daya keamanan siber pada di lingkungan Pemerintah Kota Semarang.

3.3. Konstituen

Konstituen SemarangKota-CSIRT meliputi :

a. Dinas, Badan, dan Bagian yang merupakan Organisasi Perangkat Daerah Pemerintah Kota Semarang.
b. Pemangku Wilayah Kecamatan di lingkungan Pemerintah Kota Semarang.
c. Pemangku Wilayah Kelurahan di lingkungan Pemerintah Kota Semarang.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan SemarangKota-CSIRT bersumber dari APBD Pemerintah Kota Semarang.

3.5. Otoritas

Berdasarkan Surat Keputusan Sekretaris Daerah Kota Semarang nomor 482/231 tahun 2021 tentang Pembentukan Tim Respon Insiden Keamanan Informasi (Computer Security Insident Response Team) Pemerintah Kota Semarang, SemarangKota-CSIRT memiliki kewenangan untuk melakukan penanggulangan

insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada lingkungan Pemerintah Kota Semarang.
SemarangKota-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya.

4. Kebijakan – Kebijakan

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

SemarangKota-CSIRT memiliki otoritas untuk menangani insiden yaitu :
a. Web Defacement;
b. DDOS;
c. Malware;
d. Phising;
Dukungan yang diberikan oleh SemarangKota-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa SemarangKota-CSIRT 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 SemarangKota-CSIRT merupakan layanan utama dan bersifat prioritas yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh SemarangKota-CSIRT.

5.1.2. Layanan penanggulangan dan pemulihan Insiden

Layanan ini berupa koordinasi, analisis, rekomendasi teknis, dan bantuan on-site dalam rangka penanggulangan dan pemulihan insiden siber. SemarangKota-CSIRT memberikan informasi statistik terkait layanan ini.

5.1.3. Layanan penanganan kerawanan

Layanan ini berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (hardening), SemarangKota-CSIRT 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 berupa penanganan artifak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi. SemarangKota-CSIRT memberikan informasi statistik terkait layanan ini.

5.2. Layanan Proaktif

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

5.2.1. Pemberitahuan hasil pengamatan terkait dengan ancaman baru

Layanan ini diberikan oleh SemarangKota-CSIRT berupa hasil dari sistem deteksi dini Honeynet. SemarangKota-CSIRT memberikan informasi statistik terkait layanan ini.

5.2.2. Layanan Security Asessment

Layanan ini diberikan oleh SemarangKota-CSIRT berupa identikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan. SemarangKota-CSIRT memberikan informasi statistik terkait layanan ini.

5.2.3. Layanan Security Audit

Layanan ini diberikan oleh SemarangKota-CSIRT berupa penilaian keamanan informasi. SemarangKota-CSIRT memberikan informasi statistik terkait layanan ini.

5.3. Layanan Manajemen Kualitas Keamanan

5.3.1. Konsultasi terkait kesiapan penanggulangan dan pemulihan Insiden

Layanan ini diberikan SemarangKota-CSIRT 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 SemarangKota-CSIRT mendokumentasikan dan mempublikasikan berbagai kegiatan yang dilakukan oleh unit kerja dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber.

5.3.3. Pembinaan terkait kesiapan penanggulangan dan pemulihan insiden

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

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt[at]semarangkota[dot]go[dot]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.