

RFC 2350 JatengProv-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 17 Januari 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 :

Website JatengProv-CSIRT (Dokumen Versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP Key milik Bidang Persandian dan Keamanan Informasi – Dinas Komunikasi dan Informatika Provinsi Jawa Tengah Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

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

Judul : RFC 2350 JatengProv-CSIRT;

Versi : 1.0;

Tanggal Publikasi : 17 Januari 2020;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

JatengProv - Computer Security Incident Response Team (CSIRT)

Disingkat : JatengProv-CSIRT.

2.2. Alamat

DISKOMIFO PROVINSI JAWA TENGAH

Jl. Menteri Supeno I / 2,

Semarang - 50243

Mugassari, Semarang Selatan

Indonesia

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

Telepon (024) 08319140

2.5. Nomor Fax

(024) 8319328

2.6. Telekomunikasi Lain

Tidak Ada

2.7. Alamat Surat Elektronik (E-mail)

csirt[at]jatengprov.go.id

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

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

```
mQMuBF5GTj kRCADTTlAOmJZk/WlJaOBIQluxnKXw8k4Ou5fxSWVtPcaq/ZOI+9Ti
skIwIKNSCpD7qPPlJfp7VTSaYP5Wxj1MALhUGeSXnPGbCSgxv21gjQLNmEiEOux8
JTtYVa/wRmQq7zKWGw+TmcjoMFy6qrOhfckVDEKKFnRV9/EwW7hm9h3P6nc0pvYjM
ntmvfhy/Ts4Hqyk0BZKJ3K3j8J1H8y5KC8DsBWf/vg/3AFSTNjGw9ISv+S+dpCw9
fPolpaRjHwiLWrPHNRPccEWnnjdABPlENOYAinn63dCr+Y4EnSzi5gnF6ssDDsLp
I7umrvtItHpijURFuuBmsRPLWx9JhcLCU8kvAQcP4DSqAUq6tomsWXs7KplelTSM
weR4SUieZNHM/XzP6wf/Viq3Y2PIaPnbcSvmfcXQrp/npGb6w7ShZ5s0yDlO7Yoi
sAecD5o4LAN7LImEoYniDV6xiQB8J5ftbS5mt9d4aX6ccGVtiEC6FpoWu+7BSwlF
Jb7qg3pwvzG5fIQn6nNwEuj/bVwzTXkXjcmB/tsEwYn3BnDBeZf5E3z2EhP0w1Jk
Y+108yJuZOHhyA40rTDSgSA+haQNQtuiQmc6UO8OR8+cV6vM7rGB5Owm3vTpiLyK
7HhPQHAtQHUWkGHFvjYupWjaOizz0+xF+y79hDDcma60la7LeORzrtmb3UfX9k3s
x7kxCbgoIqwWuPuG2/+COIeCHCFA0fBSnwrQC5jtNwgAlLfmZBykUHvE12LD+Nq6
ODJXdxggUKPWS/2l8OocsUS6PxWNJdXXL+CLKnGv03NZCC1vSRiz7UOGE2KkHweU
Eeew0PnAljLb0/3lc3Z3XmBSTGPbvaphR22KL6xWnY6DMUHAJovt4oeMhOefN28
rbUdywndzdjEqMLX0V8BcUfBPMOW2Y0qvwv+B1ftwD35pJGpav5cik4n9tQcSkup
ooeKWd00S+uP5eQ0CHjcREJdKRio/N0XG0MHZaqnFP4dpwCeUnpI7PzwGttrU19j
ph5c5yRF7TQ98vUUDR8IuZt1SDPiPR8aG445BtVSAy+o4j/UczM0M5I6R4iZopmT
ZLRVQXV0b2dlbmVyYXRlZCBLZXkgKEJpZGFuZyBQZXJzYW5kaWFuIGRhb3B1Zm9u
YW5hbiBjb2Vucmlhc2kpidXjc2lydEBqYXRlbmdwcm92LmdvLmlkPoiQBBMRCAA4
FiEEZmr6lnP1l4ITXIM/JbmvF/xC7B4FA15GTjkCGyMFCwkIBwIGFQoJCAACBBYC
AwECHgECF4AACGkQJbmvF/xC7B66DwD/RGzhkP6Y6Pv5iXDQAPcCa/Go6vvmLqoO
ovG3w9EfRRIA/jNlCr/+jgYpf4a8WIPY//pVvGA2+fKPFhfurPMn6V8quQENBF5G
TjkbCADLqbC5spzFWQyvMWNb6ESvGzeSS+He1lmc3hv0tt2aSXz4na7KgE3Fp99J
xqyKMRpNeMnYE9/Dwzrk6ADLt52P/oXr0FDWIKjwuMt9iizBzCOCe7zfmKxN8x6u
9so3rH3ItVqHqCGwGqNY+LWq3Lv3B6QPT8wbqMpO2qBtArTTjZEVlf0ofX/tfXPG
Jkr4ZqL9oCRYDXgB25suef/ktjBvRIFXo8UN6SpLZyXln8y6oZ0ZPjNr9S6r4KEu
0poiklbPE2/SR0iMHJxxgTsCl70fmeplJzBb5XisSUXmrQ3vdeHo5xb79JQAc5Iw
PJCHQPELYjfqRjKpQqAnQ9GcP/Q5ABEBAAGJAa4EGBEIACAWIQRmavrWc/WXghNc
gz8lua8X/ELsHgUCXkZOOQIbLgFACRALua8X/ELsHsB0IAQZAQoAHRYhBLxmngkm
QKeKGzVo7I+WtOHpGiA8BQJeRk45AAoJEI+WtOHpGiA8hRUH/jRPEFdOpoUKMxyW
ptywDFMIQz8a95adhV0Edhh730TM2OWQgX/HxjF1LwUWSlRt2M1+aHsVR5N1re+
POonROFY7f8gsW+q8Nib3ZrkF4uqZgFAKUSupCKwdhekJMWWLJ7tDGKW051Wonk5
bj3lCx+wjAS/qBmJE95IwMcnHnEZlC1qPagpdd4KLWfKz6wiXLHoLSIK1KZpbHI0
WynN0DVerIulFjwPBPgtiVbfZs9iCFCg57DG2Aw0wuGj1fFSMcI99oS4DGJ8EQLv
Ho40A9BWtmUqLSE2UYgjJPbgBOV8GkU4/ubzxeR1hmhyff60e2Tk2Vfm2wGCP2L8
YMDOFwgVvWD/Z28lQrUyc+91BHguNYzOk1gTxk1/lq1Sd4ZPf8x8NNMA+wb/fexc
vDlTJU++z1fsSwJETHKpCuLmGLCjhiAyYFWG
=/Wsv
```

-----END PGP PUBLIC KEY BLOCK-----

Kunci *PGP* Ini tersedia di Website JatengProv-CSIRT.

<https://csirt.jatengprov.go.id/app/keys/Csirt-Jatengprov-Keys.asc>

2.9. Anggota Tim

Ketua JatengProv-CSIRT adalah Kepala Dinas Komunikasi dan Informatika Provinsi Jawa Tengah. Yang termasuk anggota tim adalah seluruh staf Dinas Kominfo dan Organisasi Perangkat Daerah Provinsi Jawa Tengah adalah sebagai Agen Siber di pemerintah.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak JatengProv-CSIRT

Metode yang disarankan untuk menghubungi JatengProv-CSIRT adalah melalui *e-mail* pada alamat csirt[at]jatengprov.go.id atau melalui nomor telepon (024) 8319140 ke Dinas Kominfo Prov. Jateng yang siaga selama Jam Kerja.

3. Mengenai JatengProv-CSIRT

3.1. Visi

Visi JatengProv-CSIRT adalah terwujudnya ketahanan siber pada pemerintah Provinsi Jawa Tengah yang Handal dan Profesional.

3.2. Misi

Misi dari JatengProv-CSIRT, yaitu :

- a. Membangun pusat pencatatan, pelaporan, dan penanggulangan insiden keamanan informasi di lingkungan Pemerintah Daerah Provinsi Jawa Tengah;
- b. membangun kapasitas Sumber Daya Keamanan Siber pada Pemerintah Provinsi Jawa Tengah

3.3. Konstituen

Konstituen JatengProv-CSIRT meliputi Organisasi Pemerintah Daerah (OPD) Provinsi Jawa Tengah.

3.4. Otoritas

JatengProv-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada pemerintah.

JatengProv-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

JatengProv-CSIRT menangani insiden yaitu :

- a. ***Web Defacement***;
- b. ***Distributed Denial Of Service (DDOS)***;
- c. ***Malware***;
- d. ***Ransomware***.

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

Seluruh informasi yang diterima oleh JatengProv-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

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

5.1.1. Layanan pemberian peringatan terkait dengan laporan insiden siber

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

5.1.2. Layanan penanggulangan dan pemulihan Insiden

Layanan ini diberikan oleh JatengProv-CSIRT berupa koordinasi, analisis, rekomendasi teknis, dan bantuan *on-site* dalam rangka penanggulangan dan pemulihan insiden siber.

5.1.3. Layanan penanganan kerawanan

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

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke [csirt\[at\]jatengprov.go.id](mailto:csirt[at]jatengprov.go.id) dengan melampirkan sekurang-kurangnya :

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

7. Disclaimer

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