RFC 2350 JAKARTAPROV-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.1 yang diterbitkan pada tanggal 17 Desember 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://csirt.jakarta.go.id/

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP key milik Bidang Siber dan Sandi, Dinas Komunikasi dan Informatika Provinsi DKI Jakarta. Untuk lebih jelas dapat dilihat pada Subbab 2.8

1.5. Identifikasi Dokumen

Judul	: RFC 2350 JAKARTAPROV-CSIRT;
Versi	: 1.1;
Tanggal Publikasi	: 17 Desember 2020;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Kontak

2.1. Nama CSIRT

TEAM PROVINSI DKI JAKARTA - COMPUTER SECURITY INCIDENT RESPONSE

Disingkat : JakartaProv-CSIRT

2.2. Alamat Kantor

Dinas Komunikasi, Informatika Dan Statistik Provinsi DKI Jakarta

Jalan Medan Merdeka Selatan No. 8-9 Blok G Lantai 3 dan 13, Jakarta Pusat 10110

DKI Jakarta - Indonesia

2.3. Zona Waktu

Jakarta (GMT + 07:00)

2.4. Nomor Telepon

021-3823355 dan 021-3822357

2.5. Nomor Fax

021-3848850 dan 021-3823253

2.6. Telekomunikasi Lain

(Tidak ada)

2.7. Alamat surat elektronik (E-mail)

csirt[at]jakarta.go.id

2.8. Informasi kunci publik dan enkripsi

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

xsDNBF/Zsr8BDACw87ZpNc48y3EC/zyR1oisXWlOr6Q8mKaw8l/7++4hL5CQMlGm0KwuJRjjadpR
PLURpYYufduRoFSMAVPYlWRlca88nwPw+04a7aCSD1uO/kDMi0CFOVfT6DB4fJJ0gzGV9n+ry+GH
H1gbCCqkPnmueNo3L4l7peaTJyCwo+vyhtEaptp4wUss3wxEZUUR+c8wP2sVpGHODpnOZdJzTaSy
5cQ/51J9AO2pYhQIiM7HMDwu0KRv5PqJK/y8oi8TpHv9uP6XQZKCmA8tXar+QTHrCQ+aj/TzJyXC
2+86YFZhC6sD8sZhuU141ahIc0GD7SRsxPqnUyWvUxG8eVA8L9jW6KCsXMwv6AaCLMQO0I9HYhz
3
qgWSuqxei8krKwuqVbGzGBgJwSmT4wT+73a6cHLG5yt3GgMH80ydddhaWrpP776TAWjGLxKO1iX3
1do05Wq+KK30tBjv7srSChX0al+xc8t3P6wZs2dl1/asGabaWNGJQnjcrvRlbA+gRbPg/fsAEQEA
Ac0nQ1NJUlQgREtJIEpBS0FSVEEgPGNzaXJ0QGpha2FydGEuZ28uaWQ+wsEPBBMBCAA5FiEEjCI
u
8fgwhM70cxSVtk7xGQf/rG0FAl/Zss0FCQHhM4ACGwMFCwkIBwIGFQgJCgsCBRYCAwEAAAoJELZ
O
8RkH/6xtUm0L/AsvFQZpwjgLhUIpEI1PIxBERM3UShjCTzHTklojO4Nh2gxtqKnfR1T0PW+eq/0O
kj20Qpiu1X9MKZRiJIbeKmjoNCzZ2e5NB0lPuAd7K09LG8zMzAi0C1ZPKNqHIr0aAalb14xcH6ig
xufTEHAEbuOEygeH4XQkR8m6z8C4PcR7d5VbicAShKkwxyB1hKIO1N8w+7DoKKbAizMbWAIChOtO
UY2p+s7Wbf5DWudpaof5g9uBEyI3+M81n2UJMPtGUmax7o3KCtPon9ddama6TR8fhmTfwEHZAdu+
Oj1tehIk9NaGuLWoUIlzgsulXAYFoX54OHWZPzXaMlJ2uJBae7CVw/5RJIdxt2suAlUYrK1AaYWc
QlyGVEL5rXR/qldS+Q+m87w8e+VI4Vhp99U4HghVFq936DSK3C6LvWXfBD7p4+EBGcYkA48XRuHc
tkyB+2T5463xISmP5juJPvXrhKjKQwBs6G7m5NPAldS77cWwYNj4BOWiA4dKE1AuYwJuOc7AzQRf
2bLNAQwA36vxhz0eZQocQc3TYBpHXV2SbkFXa/cONzwXUcsysP9l9PGpY/AI03PrzC1kFHdQdiyn
7hLR5C8OeUuowyFmqgDWK97CFSkpeoaa58CqFj/xxbOz21Qwt5ZyKbq78aBlfTZoVPmYSaKOAG4r
WnKPY1RpdGCZQ+k+J2BJCPSLUF0gG1DS+nkBFDbExI6RNe21wcO9Pv0RYomXMoV3mrujGhI3SA
oU
69ijQL2k8Z85TucUXgYbH73+tV8OP/jLryAtAtpa6o3iifnGOBcJRoF2YKSNdMH88Hr98WBAeDx6

lSnmYvSPYWLrXVuMU5Zp+vrlQFZQtb4zE2WF6pW1hAO9TWNXBcGAbt3YOgFy1hJCRLTVgYZLXf
YB
el965xH0lkDsNWwxDV9NqshIfXoPHxSkDLAxcN9+4l4o2NP7RIxI0HciRB8pa9c1EdRwkIyUf/ob
GJiaNvHJPPjjCwMv0+m1uGiX9PbvrcZQxKWsZcXlfDLb/nIr7Q+igSyOvSDpKnQ/ABEBAAHCwPwE
GAEIACYWIQSMIi7x+DCEzvRzFJW2TvEZB/+sbQUCX9my2wUJAeEzgAIbDAAKCRC2TvEZB/+sbbO
g
C/4teglLzzlEKigfJ9vRjbybFccV1OcX1XM1kuOLMwOsefqpz/Z4pxwpqbi+LozLR8uuwY4tAFGP
U5zTreBiYe0swknwHAO/4seJvMR59iBDBBc+wUYuN5f/VwerhaECrYt2VGGtwySb7dFTO9uxGLGd
zo+jez3dYIoB0XQ7/Teal2lth7WNQAc/GKVD1GJAjX/2De0MN+P1AxkEvowY4uT+Lv3S8GionNBP
ZYc6tKESqUWsUNrrnUXD/gRZZrh1bv6juFpOwte9clQtySrWitetKddwRmplMo1ntCXoNZz9O4J0
hd89KvNLw8rkV16Nzkk0ruZ7qyHKRRwv8OKP5s+L2Q6NS74UhDNu8xMVGEeO3mdd+zM3wmr4Ha
Zk
y3EXPYeA4iXNWS5se8BGSR50lXmhbkh+DlsDz2uD3L/2walI2PVqzq+Neolj6vCbTrGC8MWAntYX
fO1OCOArDP1rulll4NZCrqel9wj0SivNBEiPOxq/Kxhnb/U1llGrehlxC1M=
=7nUj
-----END PGP PUBLIC KEY BLOCK-----

2.9. Anggota Tim

Penanggungjawab JakartaProv-CSIRT adalah Sekretaris Daerah Provinsi DKI Jakarta, Ketua JakartaProv-CSIRT adalah Kepala Dinas Komunikasi dan Informatika Provinsi DKI Jakarta, Sekretaris JakartaProv-CSIRT adalah Sekretaris Dinas Komunkasi dan Informatika Provinsi DKI Jakarta, dan anggotanya dari Bidang Siber dan Sandi, dan Bidang/UPT/Suku Dinas Diskominfotik Provinsi DKI Jakarta. Serta, pegawai yang menangani insiden siber / teknologi informasi di masing-masing Organisasi Perangkat Daerah di Lingkungan Pemerintah Daerah Provinsi DKI Jakarta.

2.10. Informasi/Data lainnya

(Tidak ada)

2.11. Catatan-catatan pada Kontak JakartaProv-CSIRT

Metode yang disarankan untuk menghubungi JakartaProv-CSIRT adalah melalui email pada alamat csirt[at]jakarta.go.id atau melalui nomor telepon (021) 3823355 ke Bidang Siber dan Sandi. Serta, pelaporan melalui aplikasi android ATIKA JAKARTA (Aplikasi Tiket Kita).

3. Mengenai JAKARTAPROV-CSIRT

3.1. Visi

Terwujudnya sistem keamanan informasi yang aman dan terpercaya di Lingkungan Pemerintah Provinsi DKI Jakarta.

3.2. Misi

a. Mengkoordinasikan penanganan insiden keamanan siber di lingkungan Pemerintah Provinsi DKI Jakarta.
b. Menjadi pusat pelaporan, serta penanganan insiden keamanan informasi di lingkungan Pemerintah Provinsi DKI Jakarta

3.3. Konstituen

Semua Perangkat Daerah (PD) yang terhubung dengan Koneksi Intranet Pemerintah Provinsi DKI Jakarta.

3.4. Otoritas

JakartaProv-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Pemerintah Daerah Provinsi DKI Jakarta.

JakartaProv-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya dan dapat berkoordinasi serta bekerjasama dengan BSSN / Akademisi IT Security / Principal IT Security / Ahli Security untuk insiden yang tidak dapat ditangani.

4. Kebijakan

4.1. Tipe Insiden dan Tingkatan Dukungan

JakartaProv-CSIRT menangani insiden yaitu :

a. Malware;
b. Web Defacement;
c. Phising;
d. Spamming;
e. Network Incident.

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

4.2. Kerjasama, Interaksi dan Pengungkapan Informasi / Data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, JakartaProv-CSIRT menggunakan alamat e-mail dinas tanpa enkripsi data (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi

sensitif/terbatas/rahasia dapat melalui email dinas dengan menggunakan enkripsi kunci publik menggunakan PGP.

5. Layanan

5.1. Layanan Reaktif

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

5.1.1 Layanan pemberian peringatan terkait dengan laporan insiden siber

Layanan ini dilaksanakan berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan.

5.1.2 Layanan penanggulangan dan pemulihan Insiden

Layanan ini diberikan 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 berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (hardening). 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 berupa penanganan artifak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi.

5.2. Layanan Proaktif

a. Menyelenggarakan kegiatan workshop keamanan siber kepada pihak konstituen.
b. Menyelenggarakan kegiatan Drill Test Insiden Keamanan Siber kepada pihak konstituen.
a. Menyelenggarakan sosialisasi keamanan siber kepada konstituen.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan melalui aplikasi android ATIKA (Aplikasi Tiket Kita) dengan melampirkan sekurang kurangnya bukti insiden berupa foto atau screenshoot atau log file yang ditemukan.

7. Disclaimer

(Tidak ada)