RFC 2350 JIEP-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 26 September 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Apabila terdapat pembaruan dokumen ini maka akan didistribusikan ke seluruh pihak yang terkait dengan JIEP-CSIRT

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada **csirt.jiep.co.id**

1.4. Keaslian Dokumen

Kedua Dokumen ini telah ditandatangani oleh Ketua JIEP-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 JIEP-CSIRT;
Versi : 1.0;
Tanggal Publikasi : 25 September 2024;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Jakarta Industrial Estate Pulogadung - Computer Security Incident Response Team
Disingkat : JIEP-CSIRT.

2.2. Alamat

Gedung Graha Dayaguna, Jl. Pulobuaran V, Blok JJ-4, Kawasan Industri Pulogadung, Jakarta Timur

2.3. Zona Waktu

Jakarta (GMT +07:00)

2.4. Nomor Telepon

0852 8323 4161/0852 8323 4160

2.5. Nomor Fax

N/A

2.6. Telekomunkasi Lain

N/A

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

csirt@jiep.co.id

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

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

xsFNBGbCl4wBEADWukt4OtYGw/jtVTlj2f5L/CUOiUigSsLO+h3k7beDzSNl1yNs
OVDKR/mOectptXRqIb+m7xP3fehoNRtJl7Yb+OIkcuvrCee5OPIxcMVnJMqSFIfj
CQcrecJhvP/scerNNd+kIOE7Q+yLIZk1knOUVZZ4EFRhbl27unSWzos/4cwIeN0T
ZpYxTrS5ZLLGkoquSyqSE1cE9IezGmaGlirCc/3ebNf6d6T4UkcvJ0nLCsIiYSE8
WYRTzwK8djO2kXM5EPvZHbjQfwU/H9pdFETsM3WDtc7EXczY+XPOourLJR3mjC
hY
q75SbFmP1wKR6lAG+3NEw9rXJtf+KzDIYowDg9JfFVIB36lH6zlLkY6aD8b8EREQ
kFncz16wKFfAaAERiMm7Dah2Z39zl5rZp6LGqn/WtkGOlinh6BKYwgipTRg4m321
yDwHvvUc+cccz56i7HWFmOg9vfI5DNi+bNdOjEClpydx4R9nsZelalvm9Q1zOr2G
9fVEA9iWlg2yz6mMcEgHsPAcZ98CS4ZsZc4wUCSE5lB3SOph/S8g0yqLwv7v9Ggb
2ODdRveFHqYSGkGm4omXvZKpdAI0XCA5u7sl6CaPjx+xNX7JXkMUOEdiybtcxVc8
v8tpgtT21/LhOFl/TVgkrVhHjtRtOqD2v4gSF7DbXTYXm/szbK7Wv4pPlQARAQAB
zR1DU0lSVCBKSUVQIDxjc2lydEBqaWVwLmNvLmlkPsLBlwQTAQgAQRYhBB4SWlDc
a2qH+gcZ6+aR+EFu+9T3BQJm4rgqAhsDBQkJhogEBQsJCAcCAiICBhUKCQgLAgQW
AgMBAh4HAheAAAoJEOaR+EFu+9T3y5kP/0iedh4BvYc7Go5VrLwZuL/9PjrBV2hE
7picncoXirnt3aL7M2rmuL4k2Eg62rUniMLNU2Ft1PYrCFHTMkgum2VeilQ6QXR9
tFUi3cEk/90sg5EtAllyn81bjxCe9nvCKJMWCXWBRmg+GBTFhtNHT2IPx2x5kzlb
07z+XAIKWOrNGDRVYjzDISPXTxTuAwn1oowJZheZsi/35tE/LsvIG2OPv1gEmeuC
RFfTS+E3jD2SraBY1rN1SjJWNd1OXy3d6uloKDCgl15Zo4ssdGoRa8rbm/e/Bs3z
WnurCjTsQQ9m6H9Chys7/r48BHzAK/UWI+4YqSMKPKiCWQ7pLg0eCN7P/Dt1wbJ7
NRHDfPKE4+GgrvMpQrfpkgsD6k0fGQeZ+dvTTFlVeQVsX6MKPunBFE/Yps2RtLU2
8lgkkaHKyJqukrXx5pnLj2tvBqdhVm+uijDHP2hfHAtg7pczYrUFurqIkfVRWiIa
e8TrVYbSBqwhi91JG/HE4O8EvH21hGwJIrv5suOCb9zqzq0zzeJTS1A80D/L6maQ
V8oqp698sqEKba+LzeuJTyIzanufBYK3E275X7DTHT4uU9GqYfezWwj9z/ri+XBm
I8cUi3GxQ4lNkIxFU5adI0cNeg2OGcxsDHu3UZpmSXItink9bNZKz+M3CfNMQp+3
3V1r28bBk+NHzsFNBGbCl4wBEADRSkQcTqzJYLTftnc1Z/zysli9erkba4999S4Z
dbKZI6qFPbZtWzRx9TugUCgXTB2osC7UsHe9ouSTvS6IR9bdu/Ki7liHJ2Ryvl6C
3BRg2yVJT634WO9PMkUH46bmyv8L2/iom6Z7K66wtlx4Qfjr1ncFt5spV+T/oZIA

IdeuQZH8kAV/VMymcyypA4SdWbD9nJ77GhL/OMNfCdUiOblOC773AbevcA1A79O
e
9dzBmG1N1Kd4Tw/uNa8sCRGSMAAf7wYYxS/Bq+jQbDzd7zjMT0pCpb3lVEQVKn
Hp
daimO9i03njUNWK6eyCu8czfxMX0v4xX9rwQPZi3sGWgSxVrNZxvAl1POM2olDAm
p5oWlo1hE4uPRQJ1GSaeZqx82XBrGKeId7PNkvaTbci/DuzsMKjxsudO5iJ+ax7P
JsFrsN44ir75fJZMuglnfo+b5qJKJE9BKhpm0cm0QSNW8fRv01PAu3YxnBizbH5N
kxNM3367g9LiK/xWqohlEobVBklMUG5CFRDSicRqBIMlsCSLe7dt2D3EmZyzyFpD
E/qJW0P23PynwapsdFbVVualJf03qJo6reI6Q/kfMZhsePbxbuW3DFz9lMdCFP9C
uUH8Q2btiQOpH5OBfS5WUO1vS/T7rPd1WTlwPG+TrKt3wXuIkt6hfS2wUQVpMZb
O
rsJc1wARAQABwsF8BBgBCAAmFiEEHhJaUNxraof6Bxnr5pH4QW771PcFAmbiuCo
C
GwwFCQmGiAQACgkQ5pH4QW771PeUXA//VglxfYk6Ws378DGTi2B0f9Z/HU2QVY
HF
9IIwKEbbhlmbrmT6nK8ffZamy3eV7VzzSH8QyuuNPyhrfcNaEp0hWLPhe7JDLwT3
pBhuJo/9DReZWnjR8W1McpWART5yBg7Z4P9wMdE9VH/r0Xim6zPnXx6V+7UWC
9Ui
oS5GM2zWcZl7RqrZ8IL4EYOq14f25mnB7CXtpiMtOpJA0C4T4i1nDkIEBSW8vOCH
QYCGLQ//nDxdxkG+zPkmGiMEbAFCr9gsfZG48Cqd5OJUqXGMGpzm6XumcT1fH
Wvb
OVQPR2i7kcogflS+X+Yy2q1KFVTIXno2oUYaNlOyKbIdX3W5elSZ7HQVBXMcade/
8GVc8n8UK9pAs71dZS21dPjoMQ2/LYcQ1k+rqrsA6fE9yG94e5WYl6e2sAUQTzSd
tEi5oB+HTN3e1BP4i3u3/xSnsA58w/dCGr3oVQOlK/FaXXn5xGnoe0a9zB5m3K7Q
F6Fk3dbCwX89RLTtPUUoHLjMXwll6thNRaxypu+Ht4KfZWG22TDYgoCkCsWtwfSz
6j6E4co9aEK4tOaaAduWkFfeI0qc0Y3Jp7DX9kzPQ5eJYaLCbh1RoTYOF/UPYSSh
SMwJhXf8bMoo9RHHMNHnviSKs1YWjeiAXzrRYag59SaM29lDR4n9+iVOIDlFz4Oz
mIG+CjNlyfw=
=Dt/J
-----END PGP PUBLIC KEY BLOCK-----
File PGP key ini tersedia pada: csirt.jiep.co.id

2.9. Anggota Tim

Ketua JIEP-CSIRT adalah VP IT & General Affairs. Untuk anggota tim merujuk kepada Surat Keputusan PT JIEP Nomor 095 Tahun 2024 Tentang *Pembentukan Computer Security Incident Response Team PT Jakarta Industrial Estate Pulogadung JIEP-CSIRT*

2.10. Informasi/Data

N/A

2.11. Catatan-catatan pada Kontak JIEP-CSIRT

Metode yang disarankan untuk menghubungi JIEP-CSIRT adalah melalui *e-mail* pada alamat csirt@jiep.co.id melalui nomor telepon yang tercantum pada Informasi Data/Kontak. Pada hari Senin-Jumat pada pukul 08.00-16.30 WIB dan jika terdapat hal-hal yang mendesak di luar jam tersebut dapat dilakukan penanganan

3. Mengenai JIEP-CSIRT

3.1. Visi

Visi JIEP-CSIRT adalah terwujudnya ketahanan siber yang andal dan profesional di lingkungan PT JIEP.

3.2. Misi

Misi dari JIEP-CSIRT, yaitu :

a. Membangun kapasitas dan kapabilitas sumber daya keamanan siber
b. Menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan, penanggulangan dan pemulihan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan dan kerugian
c. Menyediakan mekanisme penanggulangan insiden dan/atau pemulihan insiden yang dilakukan oleh tim penanggulangan dan pemulihan insiden siber

3.3. Konstituen

Konstituen JIEP-CSIRT meliputi seluruh pengguna teknologi informasi di lingkungan PT JIEP.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan JIEP-CSIRT bersumber dari anggaran perusahaan.

3.5. Otoritas

Berdasarkan Surat Keputusan PT. JIEP Nomor 095 Tahun 2024 Tentang Pembentukan Computer Security Incident Response Team PT Jakarta Industrial Estate Pulogadung JIEP-CSIRT, PT JIEP berwenang untuk melakukan pengelolaan insiden keamanan TI secara proaktif dan reaktif.

4. Kebijakan – Kebijakan

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

JIEP-CSIRT memiliki otoritas untuk menangani insiden yaitu :

a. *Web Defacement*;
b. *DDOS*;
c. *Malware*;
d. *Phising*;

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

JIEP-CSIRT akan melakukan kerja sama dan berbagi informasi dengan tim CSIRT/ TTIS atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diberikan dan diterima oleh JIEP-CSIRT harus dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, JIEP-CSIRT dapat menggunakan alamat email tanpa enkripsi data (email konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi pada email, data atau jalur komunikasi lainnya.

5. Layanan

5.1 Layanan utama

Layanan utama dari JIEP-CSIRT yaitu :

5.1.1 Pemberian peringatan terkait keamanan siber (*alerts and warning*)

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

5.1.2 Penanggulangan dan pemulihan insiden siber (*incident handling*)

Layanan ini diberikan berupa kegiatan menerima, menanggapi, dan menganalisis Insiden Siber.

5.2 Layanan tambahan

Layanan tambahan dari JIEP-CSIRT yaitu :

5.2.1 Penanganan kerawanan sistem elektronik

Layanan ini berupa koordinasi, analisis dan rekomendasi teknis dalam rangka penguatan aspek kendali keamanan (*security control*) baik dalam lingkup teknis ataupun non-teknis (*Policy/Governance*).
Secara umum penanganan ini dibagi menjadi :

1. Pelaporan kerawanan yang bersifat sewaktu oleh pemilik/penyelenggara sistem elektronik milik konstituen.
2. Layanan penanganan kerawanan sebagai tindak lanjut dari kegiatan audit atau *vulnerability assessment*

5.2.2 Penanganan artefak digital

Layanan ini merupakan suatu proses yang sistematis dalam mengelola dan mengamankan data digital seperti log file, data jaringan, file konfigurasi, dan berbagai jenis data lainnya yang dapat memberikan petunjuk tentang penyebab, dampak, dan kronologi suatu insiden.

5.2.3 Pemberitahuan hasil pengamatan potensi ancaman

Layanan ini diberikan berupa penyampaian kepada konstituen terkait ancaman terhadap Sistem Elektronik yang dapat muncul akibat perkembangan teknologi, politik, ekonomi, dan perkembangan lainnya.

5.2.4 Pendeteksian serangan

Tim JIEP-CSIRT memiliki beberapa sistem untuk mendeteksi apakah sistem pada perusahaan yang bersangkutan dengan *stakeholder* aman atau memiliki risiko, sehingga dapat dilakukan penanggulangan sedini mungkin.

5.2.5 Analisis risiko keamanan siber

Tim JIEP-CSIRT melakukan identifikasi, penilaian, dan prioritas terhadap potensi ancaman, kerentanan, dan dampak yang dapat terjadi pada sistem informasi suatu organisasi. Tujuannya adalah untuk memahami tingkat risiko yang dihadapi dan mengembangkan strategi mitigasi yang efektif.

5.2.6 Konsultasi terkait kesiapan penanganan insiden siber

Tim JIEP-CSIRT membantu organisasi dalam meningkatkan kemampuannya dalam merespons dan memulihkan diri dari insiden keamanan siber.

5.2.7 Pembangunan kesadaran dan kepedulian terhadap keamanan siber

Tim JIEP-CSIRT akan memberikan edukasi dan pelatihan yang komprehensif untuk membekali konstituen dengan pengetahuan dan keterampilan yang dibutuhkan untuk mencegah terjadinya insiden keamanan.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke *csirt@jiep.co.id* atau melalui aplikasi ITSM(*itsm.jiep.co.id*) dengan melampirkan sekurang-kurangnya :

a. Identitas pelapor;
b. Tipe laporan;
c. Waktu terjadinya insiden;
d. Tipe insiden;
e. Deskripsi insiden disertai bukti (*screenshoot*, domain name, URL, email dll).
f. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

a. Layanan yang disediakan oleh JIEP-CSIRT sesuai dengan ruang lingkup dan jenis layanan sebagaimana tercantum dalam Dokumen RFC 2350 JIEP-CSIRT.
b. Segala dampak atau konsekuensial yang timbul dari pemanfaatan layanan JIEP-CSIRT menjadi tanggung jawab Konstituen sebagaimana tercantum dalam Dokumen RFC-2350 serta diselesaikan sesuai hukum yang berlaku di yurisdiksi tempat JIEP-CSIRT beroperasi.
c. Ketentuan terkait kerahasiaan dan privasi data dilakukan berdasarkan ketentuan peraturan perundang-undangan yang berlaku.
d. JIEP-CSIRT hanya dapat menindaklanjuti laporan yang telah memuat informasi secara akurat dan lengkap.
e. Layanan JIEP-CSIRT bersifat dinamis dan dapat berubah sewaktu-waktu sesuai dengan kebijakan yang berlaku.