RFC 2350 WASKITA-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 30 Mei 2023.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada.

1.3. Lokasi dimana Dokumen ini bisa didapat

Hanya tersedia di Internal PT. Waskita Karya (Persero) Tbk pada Portal Internal Waskita (Beranda Kita) yang dapat diakses melalui https://ptwaskita.sharepoint.com/sites/BerandaKita/csirt

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP Key milik WASKITA-CSIRT. Untuk lebih jelas dapat dilihat pada Sub bab 2.8.

1.5. Identifikasi Dokumen

Dokumen memiliki atribut, yaitu:

Judul	: RFC 2350 WASKITA-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 30 Mei 2023
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

PT. Waskita Karya (Persero) Tbk. - Computer Security Incident Response Team
Disingkat : WASKITA-CSIRT.

2.2. Alamat

Jl. MT Haryono Kav No. 10 Cawang Jakarta Timur 13340

Zona Waktu

Jakarta, Indonesia (GMT+7)

2.3. Nomor Telepon

(021)8508510/20 ext 247

2.4. Nomor Fax

-

2.5. Telekomunikasi Lain

-

2.6. Alamat Surat Elektronik (E-mail)

csirt@waskita.co.id

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

Type : OpenPGP

Key Length : 4096

Fingerprint : 14D7759EA2C1DB7CE4C012FFA4B2E4149E910895

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

mQINBGR2wPkBEACpj2GQqahyK9eVzltn6/ARckj25LdKwhs2ehFzPY+2dCBO519S
FdL5diFF1AV/KpbIbY+lqec62TCXVmYEMc2gvSbaX0Od+ADcuXko3FMSyRPkpQ8z
K/YRKTHiDKcJJ1W1VFCdPuwh5rncqeN45HduKvVK7efFnwpaPHB1Xc86kBJqKwMr
Ux8jR3n3pniM969jzT+OVFVeg+9HEeXQWuXqx5+XzmqJa5/2Uwl66JRTnpLBsWjS
CnnYTIXRW9U3J+0iEvulW8AXuk5us6cSnQHndqGRW9AVULjXCGhbhM5y6EVFFRRt
d+GJ+tSqThzhzNvK8H2XVQP+Qk7RdOl2I7AwSvriJiQbP4v3bjqaN68v0sRNpJDh
LC69AHaehdKm/fr5wKQ1fya+5yfWvV8vLLtCx5OoFYjeSIG4nTz0lfd7boLsJQlk
KM/lGPNjGDKazgNsfF+ir7OzL8nhOikoszEslpAAK/1cxJ5p0IOlyKCPvovSEAAz
IpVvpfrNok08xpx1LEboIdlviS9fOoIlGiVpIgv9gDxICIqUBaCrlbVM9Pi1hVna
W08ZUTX2357eTey+wRe55gx/oU57uD8dwmciZh0s3ImdvHNmfrH9hK576f6Wnp3O
sWsb02jhptRl8rH2TJQgB0kpDndulBqGZTuNuHx9psMvzcQySQdZLNe1YwARAQAB
tCNjc2lydC13YXNraXRhIDxjc2lydEB3YXNraXRhLmNvLmlkPokCVwQTAQgAQRYh
BBTXdZ6iwdt85MAS/6Sy5BSekQiVBQJkdsD5AhsDBQkB4phXBQsJCAcCAiICBhUK
CQgLAgQWAgMBAh4HAheAAAoJEKSy5BSekQiV3aUP/1XEXGXW8PK0/ux7I3i2dlz5
w3QaHq48dtOmzdgFA5sdO8P/oAzGvXAzwzBX3pi/MDJCbokF1kWy2Hb7eKiB3Aht
U+Mu5iZfIkh7pgIgqGes4ggMnf3b+343Hr38zgMUXku0FUigijb+X6NvWwXq+JhK
axh5wnzTnZuvCew4HI6HtyxvNl8Wwl1MraNgwaWKlf9xvNLFm7KliC5OhWVnqQMP
igflk/oXls+2COqdwi+jeA8p2AhYs/GXMBQIpgaPWH3ghxBWjQkAjyOMRAD/LUsr
6D2NDIib0vIRjv6zCnX72Q7+UukJDwYoV/ttrR1XuE6C32B4ciQ8PACN/T7VB8hL
itUQrixGhkMUZSfBzir/5ZW1Af+OyrZk3pZWYMvXadLpryNLeyKUQx0SMdERVa6u
iz8hRhRWGIDnInSmAm1TwsHBoWdZhHHmCFwL6bPIkrtFffn0DAhtEAjJGLxDMPCh
1jCbA5q36P2csU5I18hR+1q+9rvatEZAX43LxVQWZBTcYd9NUR6NEOHZYASXz8x+
5nLzB9p+SzwV97nu4+zRjF6UbyvJW+Q1gQuXw7PAk4FA9wBl9ToJYuM040MeeY0U
mx1GW+WOPypZi24Q6rNYRp0dgCKJ/zgrfc6CZGyj4CH+VwrixJ0WHA3xQyqXKnVk

CIP1WYg0hPSTeCYV4ylRuQINBGR2wPkBEACh94KCFTzjlNYKWgXqtnrjiX9hNC1U
RH/4nxUGxG5UDhbJILBrGLtuTL9mvFHJWDBP/MKQ/vFci9VSy3PwMVvub6ZWccOm
IhJs6MIXDGnmLoqV7C8npWDDDWnBJOjlOTAHM/lV29B58X/Bxmok6ia0FHCqm8qp
+23llgXINOD+Kcl0Xrdl+EOZi/E8Qq1/a/IiR1GVZO6IraHqPUJpAHmaYe8eFk9b
2K6BolqF4y9F/M+O0ABKN05NWH3MDaQBe6snROp94rcqZPvCm39smOuZ3Rws5Hl4
cCOujwrTxBeyymqFdDEwM7x0SNaaelufP17xOV9B3CpAws+QUGfs74ezYUovG8Lm
mHjULXQV7kWeGJFyxx3Kj3B7KVVDE5uAwJ7Rj1hGfzg6M4F8GALw7QMNVQi+Gp5
E
Sw8CkmapDwG0jRmbfRhp2+TF3mmexp5NrMQQntAtIgwTwH/DppwQo44TMgXczx1y
Bl9m9c3l2OLFsGBbrNaR41/AFl8UuZcDv0PUMwfsfBTgT9TmcWiMP+K8LPwPBdjh
G+1REMskIBTSsmLQGRdmrEI41Az0OSps2LjdyFK1OEY6sXXM98jZ/p+mJRMeyRTb
kR35tJamqbwn5rSXYHQSMKtjJ7eoGPGUxviesSE5OmiUMB8aSheSHgzr1ZhOIzTG
sjJ6pB4aUofsEQARAQABiQI8BBgBCAAmFiEEFNd1nqLB23zkwBL/pLLkFJ6RCJUF
AmR2wPkCGwwFCQHimFcACgkQpLLkFJ6RCJX5HA//dLIYQg8PBO0UGFYP4NV0fTfn
PoQEtDINwuVTWmkQkM1D4ppuCju3p78PdT1WSNSTKB2s09GYKNiDORocMcv875h
W
tMgK1XmWgUCXxSABcIao13WPbEy+5B9/eOs50BrAEhdIVJ2uGf6sp7vUgmHwp7/b
P3bcbUBqNlLpyzEu13NMitii5gnXLOd50EhjFcDyRN63jzV8ZyZXMzzD8/YqFP/2
S492OHWmB1EwQTmRs5atxUkUgCLt9AFPdF8rd40LsDzjObUIxFmYe5KZTSSWkAwI
ikqCmzS5nMZrrhEgRoZnYgwWH67MDHdLlIzRwZWiMQzU2pnWyVmeL/mZbPyktcui
eDeQHLZgGwPm1K7lIiETqK/6NOH5AYF66FZ2QpjXxx7kCcwIPtdp91koJLabZltY
GaJhmsbcrnSOTujaT4KVTaN6dNQBFR3noqlIep3KqUq8WfLzgRtFVyNk9S1NCR9k
2g6llmrUbOU5FCkxDinssa1oLjBS9XEg2QIHVCs7nacPLvNYUxVVQudbRB8MntQG
TXky61feaBisL4ITRrk5gP7gFWFKWalSkmqPNbXXvNLetgybHdGJZuWijE93mRJW
ycNLZOmiR3/21jqoim99LNDxS0VnX+kGviXJwK3rG+ldCyclaFUz68psVTvieF8n
ljNkOH1h2szDZfOcgjM=
=oofp

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

2.8. Anggota Tim

Ketua WASKITA-CSIRT adalah Senior Vice President Transformation Digital & System Development Division, Wakil Ketua WASKITA-CSIRT adalah Vice President Transformation Digital & System Development Division, serta anggota

WASKITA-CSIRT adalah seluruh anggota IT Operation & Data Analytics Department, pada Transformation Digital & System Development Division PT Waskita Karya (Persero) Tbk.

2.9. Informasi/Data lain

Tidak Ada.

2.10. Catatan-catatan pada Kontak WASKITA-CSIRT

Metode yang disarankan untuk menghubungi WASKITA-CSIRT adalah melalui media seperti berikut:

- E-mail : csirt@waskita.co.id
- Telepon: (021)8508510/20 ext 247
- Operasional WASKITA-CSIRT pada hari kerja, Senin s.d Jumat, Pukul 08.00 s.d. 17.00 WIB.

3. Mengenai WASKITA-CSIRT

3.1. Visi

Visi WASKITA-CSIRT adalah mewujudkan keamanan siber perusahaan yang handal.

3.2. Misi

Misi dari WASKITA-CSIRT, yaitu :

a. Mengidentifikasi kerentanan keamanan siber perusahaan secara menyeluruh.
b. Meningkatkan respon aspek keamanan siber kepada seluruh pegawai PT Waskita Karya (Persero) Tbk.
c. Meningkatkan mutu layanan IT PT Waskita Karya (Persero) Tbk. dari ancaman siber.
d. Melaksanakan implementasi Sistem Manajemen Pengamanan Informasi berdasarkan ISO 27001:2013.

3.3. Konstituen

Konstituen WASKITA-CSIRT meliputi :

Seluruh pegawai kantor pusat PT Waskita Karya (Persero) Tbk yang menggunakan layanan teknologi informasi yang berjalan dalam Infrastruktur teknologi informasi milik PT Waskita Karya (Persero) Tbk.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan WASKITA-CSIRT bersumber dari Perusahaan.

3.5. Otoritas

- Mengidentifikasi dan mengatasi celah keamanan, menerapkan kebijakan keamanan, serta melaksanakan tindakan pencegahan dan deteksi terhadap serangan siber pada perusahaan.

- Melakukan tes penetrasi atau serangan simulasi terhadap sistem dan jaringan perusahaan dengan tujuan untuk menemukan kelemahan dan kerentanan yang dapat dieksploitasi oleh penyerang serta memberikan rekomendasi untuk memperbaiki keamanan.
- Memantau dan menganalisa aktivitas jaringan, sistem, dan aplikasi perusahaan untuk mendeteksi segala ancaman keamanan dan serangan siber pada perusahaan.
- Merespon dan menangani kejadian keamanan yang terjadi pada perusahaan dengan melakukan investigasi, memulihkan sistem yang terkena dampak, serta mengambil langkah-langkah untuk memperkuat keamanan dan mencegah kejadian serupa di masa depan.
- Terlibat dalam mengembangkan kebijakan dan pedoman keamanan perusahaan diantaranya merumuskan kebijakan, memperbarui panduan keamanan, dan memberikan rekomendasi untuk meningkatkan keamanan siber secara keseluruhan.
- Melaksanakan program pelatihan dan kesadaran keamanan siber kepada karyawan perusahaan.
- Mengkomunikasikan eskalasi penanganan insiden dengan BSSN

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

WASKITA-CSIRT melayani penanganan insiden siber dengan jenis berikut:

a. Kerentanan
b. Serangan insiden malware
c. Serangan insiden social engineering (phising, SPAM)
d. Insiden web defacement (XSS, SQL Injection)
e. Serangan terkait jaringan (Insiden DDoS, Buffer Overflow, DNS Spoofing)

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa WASKITA-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 Utama

Layanan utama dari WASKITA-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Memberikan peringatan kepada konstituen tentang adanya ancaman atau sedang terjadi insiden keamanan siber;

5.1.2. Penanganan Insiden Siber

Penanggulangan dan pemulihan Infrastruktur IT beserta layanan IT jika terjadi insiden keamanan siber.

5.2. Layanan Tambahan

Layanan tambahan dari WASKITA-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berupa identifikasi, analisis dan memberikan rekomendasi tindakan perbaikan terhadap kerawanan atau kelemahan dalam sistem elektronik PT. Waskita Karya (Persero) Tbk.

5.2.2. Pendeteksian Serangan

Layanan ini berupa pendeteksian serangan siber secepat mungkin menggunakan perangkat security agar respon dan tindakan dapat diambil untuk mengurangi dampak dan melindungi aset perusahaan.

5.2.3. Analisis Risiko Keamanan Siber

Layanan ini berupa identifikasi, evaluasi dan pengelolaan risiko keamanan yang terkait dengan keamanan siber perusahaan.

5.2.4. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini bertujuan untuk membantu mempersiapkan dan meningkatkan kemampuan dalam menangani insiden keamanan siber yang berupa evaluasi, perencanaan dan pelatihan.

5.2.5. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini berupa peningkatan kesadaran dan kepedulian konstituen terhadap keamanan siber (security awareness) melalui kegiatan-kegiatan kampanye dan sosialisasi/literasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan melalui email ke csirt@waskita.co.id dengan melampirkan sekurang-kurangnya :

a. Foto/scan kartu identitas
b. Bukti insiden berupa foto atau screenshoot atau log file yang ditemukan
c. Atau sesuai dengan ketentuan lain yang berlaku

Pelaporan insiden keamanan siber juga dapat dilakukan dengan menggunakan aplikasi IT Service Management Waskita yang dapat di akses pada alamat https://servicedesk.waskita.co.id (hanya dapat diakses dari dalam jaringan waskita)

7. Disclaimer

a. Bagi konstituen, sampai saat ini WASKITA-CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada perangkat kerja yang bersifat dinas.
b. Terkait penanganan jenis malware tergantung dari ketersediaan dan kehandalan tools yang dimiliki WASKITA.
c. Apabila dibutuhkan, segala konsekuensi hukum yang disebabkan oleh insiden keamanan siber akan diteruskan ke institusi penegak hukum sesuai dengan peraturan perundang – undangan yang berlaku.

Jakarta, 30 Mei 2023

Ketua WASKITA-CSIRT

Shastia Hadiarti