

RFC 2350 KBUMN-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 24 Juni 2022.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :

<https://csirt.bumn.go.id/rfc2350.pdf> (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen tersebut telah ditanda tangani dengan PGP *Key* milik KBUMN-CSIRT. Untuk lebih jelas dapat dilihat apda Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 KBUMN-CSIRT;

Versi : 1.0;

Tanggal Publikasi : 24 Juni 2022;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Kementerian Badan Usaha Milik Negara – Computer Security Incident Response Team (CSIRT)
Disingkat : KBUMN-CSIRT.

2.2. Alamat

Gedung Kementerian BUMN
Jalan Medan Merdeka Selatan Nomor 13
Jakarta Pusat 10110

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 2993 5678

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak Ada

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

csirt@bumn.go.id

bidang.ti@bumn.go.id

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

Bits : 4096

ID : 0x8E4EF822

Key Fingerprint : 6C66250F95773F7C262681E3EB5FEC5B8E4EF822

Blok PGP Public Key Misalnya :

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

```
mQINBGKZj08BEADbaUW9ozGp97/8dz6lvREcxDIFHuO7Bo3f591iz1Plyn1YP8zO
WueulA4RvWz0rnf7SctsPv3+6jEjwJhZa8bwJMLiXU/ZBWkioQWZgXuXG21MxDH
esLkNnvdpXde8e9aIVON4bffp4jP9x75xQQZ1FbAmnVT5I5ZjeOPZEMS8TxZx+xiJ
g7x7yTMrQFrCliCK2oN0zdawAV1VaYbu7H2BWboF8ESi5563z9KkStzHU1sL338O
x9oe4HNV1IOESowzKrw2nb5h7QhTHoBuAgm9+XFsfHdjZm2nea1pQJS+vDITCS
f
OFQsk/NiTOJ9DxGTgImwzWpYEv93t9QGTXUBI1BrohWrP7UqLr7bBgsrtF7qcOPu
Ughcf+iywTPMbrTeqNEzihBQ92E9K0rYoZUqP3q6O7DIg8CyhjA2yHg9WrfBjUe0
K16VdZU389Hmw98lekiYORZwixdKrVmUbFbKCJCXU/pi7fj9c20AWEqf2priKuH2
wFRctquDn/qZHq4Yo9fjwgSwY0D49LmflKlqHEuxJ/thN1WhFIBeBJV1x6XjoAL
rBFNQdPeDfVtbp3IL91JvB7ShbXY0XukR7PMzAwKaX70tU1cC+hr7midYcVN/Dt4
xG0WUwnBLAniO1ARp7TL0XLc/DjWaf8GQfWV5I2QVs5315++6iTUMoRqQARA
QAB
tB5jc2lydCBryNvtbiA8Y3NpcnRAYnVtbi5nby5pZD6JAicEEwEIAEEWIQRsZiUP
IXc/fCYmgePrX+xbjk74IlgUCYpmPTwblwUJA8O+gQULCQgHAGliAgYVCgkICwIE
FglDAQleBwlXgAAKCRDrX+xbjk74lpWGEACrFsj14d346mQTUJ/KTi8iq5SzxSBH
awZzvvCld5d3dxeV55uEZKhDa6q5NxrLVL08StnH4VvKCpqqKvJyWPTuN5prabjR
n3/emTZ4KDFDTnnFmz33GPDcpxzMEG0tiEDGfVYKE2vRkyBt1EXCwUJDFgGkL+
FE
tMQKbX3zDYkolyqhSumbv8cSmkebRpWtXy9XPzW5p70c8E5AA7HZTqkXmvtJkfx
ciE0oF4tQsMueA1hkV0DANu1WZsY/NX+m4LEYnRF3Jr/LLzNcqhyGIQjTh4DLu
KpYBz2d/kiOkmMuLGF9K6sMJQqogSGBTxVCGOKJ13PQ87cmCdsrt5pLQe5Hm
SXT
gSf9AsdQWsxKO1jG5Je584fgirEKMXRm3InhQQsLs3YMPY1OU6iHz2+q657XsEv
```

z4X7PQHxOxnb/pW1D8S/jdxkunZu2+qcHzg+tg6qAINGyKXVpl9FoOkLZcKwISDW
JPN+0/LUzOV8BdJIC6XicdeT+0aGccMyOPx9sBSC0QO5iQntdVSzXx9VvhEMMxL
V
DM7pWZqapSIVC86M2Jc8WlolARe3AmBH7EaNAixHm6ZDP1BdLzEWdG7Oe9Ys
RPs+
zY/yvmwjmTED+FQDq6YKCKNAV7B09kk1xKYaW9uUEslQe+YUd6AnF8pwOPpD
Tx9C
qrtko0YtJ+c55rkCDQRimY9PARAA238EZ6Bb9bo59qi54dJtQowOI40vCS0ndo+N
Q6zIzhR3BVol87sry3Eo+b1+BRWz6yobsYBqtdIOKKusZipyM4dV+5BdLvSXVbWD
GgG0oTAnzGtShFOJNJ3JWuWMTsckuxwQADAZqXfKXHoA6cAmGJ2UP159sVdH
5M35
yuxwL8nzRU0zT9QWwQ+VgZrNMkDgjssMDvbDoooAkBBZauLGN64CLR8zCBBP
bLBM
54fLNutPAdV9hXa30dmiJutvD+FPsSneSrZkPi+kqYqEikVM234v8EpPp08ofxSz
DPUes/iLeTNuxRtMfGdDAqX9VdUcgNkQLQ8/tNek/4XMCsK8RiJy6iJGDEonAls+
zwlkvclL6W0n5uJurWf9Y+Jhaw39wKuwhEOG6kzH0DcmmCYkov1bMltAOhymlp3
H
7hMsBYT0n2KWU8Bj3bhp7+LTc/aBZk/W9e6sbabZ8Nc24Y2Pc8WudpgjDL2REbL
y
SljqTvMV3kfkM+gluHZNmn/CMMkXrlsCs8kNQIKkNnjJRDVcj0lcvEqIf38IUp1c
A+Cki8z3OI5QUq/47ntPwRV1DKX8WEMM9IDMykWSSFknxF3OZkzwYuV06obtVT
yO
O2OCNqLIdF7rbQY+62TIXHI1cDVa/6k8niG+q4rZCazWPHS3JTfo1es9XSE4iNCv
B4inLucAEQEAAyKCPAQYAQgAJhYhBGxmJQ+Vdz98JiaB4+tf7FuOTvgjBQJimY9
P
AhsMBQkDw76BAAoJEOf7FuOTvgisGkP/joth6xfC2RQDE5PtVjBiwcuFEyKnnAC
vp58JUWh3bjVe3EgF2obAcGEtJkeby89yKI3hioPlxK0cn7dXRnOHV4aWBTNNMB
M
um1O44jCmAqIAPi+R2WHrjRc0U9M4ad6CfnMZUaMMq0HuVaQirttTLQF51U3GDf
U
xtdiE4jEqHqilUiM1mh/rD/YOgjGT/RaZ7xjZxMTLfkpDo0A4I5uSluKzAOMDDh2
XXnJ+i0QjodzjAljaTYTcaYtPO8RJPjWSpkNxKICzal1NykrAKSYGIqsSzvLRKY
L8xPxjE4d0icActCoAgTInBodE5SKtqSTiFN9nMW/XmxU5g6J4ttoPbsCXbu+0pB
b4W6D7EH+wUq+QhtTlbCw/6RIHst8BhXJDI9dHDOBkt3PF3+oWo3QzSKY18/Qq
DG
05nGU5/NpAWZ4eiWuzMspbVC5TZN/flAkc5drH4DW7mkZiO4bdITqdEviW3IBo9N
tZm7fliddVJbxwr6RcmqgS/fpjOjl/UDaZCYf73ZVEQIxM9VbpFcFv0TPuF0IHn
L8zYhOCK8Eai727IPuSM77Rf5sL2LABn3k6cEltp6H5aptUPaf6hLEtxibb/wmiV
ShUsPas0x6pj1DQtzYvIFEKPNqzAPKUYLgCsqUb2TN5hPc34mQr0Ud64S/+ziLrD
iUrplJYto8/w
=VFTa
-----END PGP PUBLIC KEY BLOCK-----
File PGP key ini tersedia pada :
<https://csirt.bumn.go.id/publickey.asc>

2.9. Anggota Tim

Ketua KBUMN-CSIRT adalah Asisten Deputi Bidang Teknologi dan Informasi Kementerian BUMN. Yang termasuk anggota tim adalah seluruh staf Keasdepan Bidang Teknologi dan Informasi sebagaimana dalam SK Menteri BUMN Nomor SK-142/MBU/07/2022.

2.10. Informasi/Data lain

Tidak Ada

2.11. Catatan-catatan pada Kontak KBUMN-CSIRT

Metode yang disarankan untuk menghubungi KBUMN-CSIRT adalah melalui *e-mail* pada alamat csirt@bumn.go.id atau melalui Nomor telepon (021) 2993 5678 Ext 1010 ke Keasdepan Bidang Teknologi dan Informasi yang siaga selama Senin – Jumat, 07.00 – 17.00 WIB (tindaklanjut pada jam kerja)

3. Mengenai KBUMN-CSIRT

3.1. Visi

Visi KBUMN-CSIRT adalah terwujudnya pengelolaan keamanan informasi di lingkungan Kementerian BUMN sesuai dengan prinsip keamanan informasi yaitu untuk menjamin ketersediaan (*availability*), kebutuhan (*integrity*), dan kerahasiaan (*confidentiality*) Aset Informasi Kementerian BUMN.

3.2. Misi

Misi dari KBUMN-CSIRT, yaitu :

- a. Melaksanakan pengelolaan keamanan informasi sesuai prinsip keamanan TI;
- b. Membangun kompetensi dan kesadaran sumber daya manusia di Lingkungan Kementerian BUMN terkait keamanan informasi;
- c. Melakukan koordinasi dan kolaborasi mengenai pengelolaan keamanan siber dengan pihak terkait; dan
- d. Mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi.

3.3. Konstituen

Konstituen KBUMN-CSIRT meliputi Seluruh Unit Kerja di Lingkungan Kementerian BUMN.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan KBUMN-CSIRT bersumber dari Unit Keasdepan Bidang Teknologi dan Informasi

3.5. Otoritas

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

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

KBUMN-CSIRT memiliki otoritas untuk menangani insiden yaitu:

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

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

KBUMN-CSIRT akan melakukan kerja sama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber.

Seluruh Informasi yang diterima oleh KBUMN-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, KBUMN-CSIRT dapat menggunakan alamat e-mail dan telepon.

5. Layanan

5.1. Layanan Reaktif

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

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

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

5.1.2. Penanganan Insiden Siber

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

5.1.3. Vulnerability

Layanan ini dilaksanakan oleh KBUMN-CSIRT berupa pengukuran *Vulnerability* secara periodik di Kementerian BUMN

5.2. Layanan Proaktif

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

5.2.1. Pencegahan dan Konfigurasi Perangkat dan Infrastruktur

Layanan ini dilaksanakan oleh KBUMN-CSIRT berupa langkah pencegahan dengan konfigurasi perangkat dan infrastruktur TI di Kementerian BUMN.

5.2.2. Deteksi Ancaman

Layanan ini dilaksanakan oleh KBUMN-CSIRT berupa monitoring secara berkala atas transaksi data dan kemungkinan ancaman di Kementerian BUMN.

5.2.3. Penetration Test

Layanan ini dilaksanakan oleh KBUMN-CSIRT berupa uji penetrasi perangkat di Kementerian BUMN.

5.2.4. Audit/Assessment Keamanan TI

Layanan ini dilaksanakan oleh KBUMN-CSIRT bersama dengan Konstituen berupa Audit Keamanan TI secara berkala.

5.3. Layanan Manajemen Kualitas Keamanan TI

5.3.1. Manajemen Risiko

Layanan ini dilaksanakan oleh KBUMN-CSIRT bersama dengan Konstituen berupa manajemen risiko TI di Kementerian BUMN.

5.3.2. Evaluasi Keamanan TI

Layanan ini dilaksanakan oleh KBUMN-CSIRT bersama dengan Konstituen berupa Evaluasi Keamanan TI baik dari sisi SDM, Anggaran, Pelaksanaan Layanan, dan tugas KBUMN-CSIRT lainnya.

5.3.3. Pelatihan/Sosialisasi Keamanan TI

Layanan ini dilaksanakan oleh KBUMN-CSIRT berupa pelaksanaan sosialisasi/pelatihan kepada Konstituen terkait Keamanan TI di Kementerian BUMN.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@bumn.go.id dengan melampirkan sekurang-kurangnya:

- a. Foto/*scan* kartu identitas
- b. Bukti insiden berupa foto atau *screenshot* atau *log file* yang ditemukan
- c. Apabila dihubungi bersedia memberikan data-data terkait kebutuhan penyelesaian insiden

7. Disclaimer

KBUMN-CSIRT memberikan respon terhadap pelaporan insiden pada jam Kerja (07.00 – 17.00). Namun, terkait waktu penyelesaian insiden siber bervariasi sesuai dengan kondisi situasional insiden yang dihadapi.