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 2.0 yang diterbitkan pada tanggal 19 Agustus 2025.

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 pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 KBUMN-CSIRT;
Versi : 2.0;
Tanggal Publikasi : 19 Agustus 2025;
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

082312126860 (helpdesk IT KBUMN)

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak Ada

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

csirt@bumn.go.id

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

Key Fingerprint : 844AE1A6E8933B41A1A899AA5149622F14973D61

Blok PGP Public Key Misalnya :
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEaJ0+/RYJKwYBBAHaRw8BAQdAk1l9sXTt20CW8/NoogOTsSZKWN79j23W
WOzh
1J+rtYC0HktCVU1OIENTSVJUIDxjc2lydEBidW1uLmdvLmlkPoiZBBMWCgBBFiEE
bCI/0Qb4DdypRUnFPDpPwc4w/zkFAmidPv0CGwMFCQWlGlMFCwkIBwICIgIGFQ
oJ
CAsCBBYCAwECHgcCF4AACgkQPDpPwc4w/zlK2wEAjXEfq46AXItJT7VYntZcfko
J
6jFJe0RxJ9Drwi37jgQA/0edHPGWw26jTaWjDIzu7++WkMmDpr8f10G6YHxemFM
B
uDgEaJ0+/RIKKwYBBAGXVQEFAQEHQJRVdD1wH3CvApGTgGrlHtW5ZUQN9JC
CfgIA
HlReUWFoAwEIB4h+BBgWCgAmFiEEbCI/0Qb4DdypRUnFPDpPwc4w/zkFAmidP
v0C
GwwFCQWlGlMACgkQPDpPwc4w/zngAwEAsNYsQI80VGzlM24xlU3RCJ1Zlj8FM
NQO
sYJJ6vEhdWYA/juXgY0gNsH37yeYhdrZgATawyx9MmdtMlzTR6d+qeAA
=+w6k
-----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 staf Keasdepan Bidang Teknologi dan Informasi dan perwakilan dari Biro Hubungan Masyarakat dan Fasilitasi Dukungan Strategis sebagaimana dalam SK Menteri BUMN Nomor SK-14/MBU/DSI/04/2025 tanggal 14 April 2025 tentang Perubahan Kedua atas

Keputusan Menteri Badan Usaha Milik Negara Nomor SK-142/MBU/07/2022 tentang Kementerian Badan Usaha Milik Negara *Computer Security Incident Response Team* (KBUMN-CSIRT)

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 seluler *Helpdesk* TI 0823-1212-6860 yang siaga selama Senin – Jumat, 07.00 – 17.00 WIB (tindak lanjut 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; dan
c. Mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi dengan membangun kerja sama dan kolaborasi dalam pengelolaan keamanan siber dengan berbagai pihak.

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 APBN Kementerian BUMN unit Keasdepan Bidang Teknologi dan Informasi sesuai dengan tahun berjalan

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 Monitoring dan Aksi

Layanan monitoring dan aksi menyelenggarakan fungsi yang terdiri dari:

5.1.1. Fungsi Monitoring

i. Melakukan pemantauan terhadap jaringan, sistem, dan aplikasi untuk mendeteksi aktivitas yang mencurigakan atau anomali;
ii. Menggunakan alat pemantauan jaringan dan sistem seperti SIEM (*Security Information and Event Management*), IDS/IPS (*Intrusion Detection/Prevention System*), dan alat pemantauan log;
iii. Menganalisis log sistem dan peristiwa keamanan untuk mengidentifikasi tanda-tanda kompromi atau serangan;
iv. Mengidentifikasi pola dan indikator ancaman (*Indicators of Compromise – IoCs*) yang dapat menunjukkan adanya aktivitas berbahaya;
v. Melakukan monitoring pendeteksian serangan;
vi. Menyampaikan pemberian peringatan terkait keamanan sisber kepada para pihak terkait; dan
vii. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan monitoring.

5.1.2. Fungsi Tanggap Insiden

i. Membuat, memelihara dan mengevaluasi standar operasional dan prosedur proses tanggap Insiden Siber;

ii. Memberikan asistensi dan/atau bantuan terkait tanggap Insiden Siber kepada konstituen KBUMN-CSIRT;
iii. Melakukan pemilahan (*triage*) Insiden Siber sesuai kriteria yang ditetapkan;
iv. Melakukan penanganan artefak digital;
v. Melakukan akuisisi dan preservasi data dan informasi yang diperlukan dalam proses investigasi atau tanggap Insiden Siber;
vi. Membuat laporan proses tanggap Insiden Siber yang dilakukan
vii. Melakukan pengelolaan, pendokumentasian terhadap laporan tanggap Insiden Siber;
viii. Membuat publikasi terkait dengan *best practices* proses tanggap Insiden Siber;
ix. Melakukan analisis terhadap Insiden Siber yang terjadi yang diperoleh dari hasil kerja sama ataupun dari *news feed* yang ada di media sosial untuk menjadi *lesson learned* kepada konstituen KBUMN-CSIRT dan forum berbagi koordinasi dan komunikasi KBUMN-CSIRT; dan
x. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan tanggap insiden.

5.1.3. Fungsi Uji Penetrasi

i. Melakukan pemindaian kerentanan secara berkala terhadap aset konstituen KBUMN-CSIRT;
ii. Mengidentifikasi kerentanan dalam sistem;
iii. Menilai dampak potensial dari kerentanan;
iv. Melakukan penanganan kerentanan sistem elektronik;
v. Menyusun laporan kerentanan secara berkala berdasarkan konstituen KBUMN-CSIRT;
vi. Melakukan reviu terhadap laporan kerentanan; dan
vii. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan uji penetrasi.

5.2. Layanan Penanganan Kerentanan

Layanan penanganan kerentanan menyelenggarakan fungsi yang terdiri dari:

5.2.1. Fungsi Peneliti dan Penerima Laporan Kerentanan

i. Mengidentifikasi kerentanan yang dieksploitasi dan laporan kerentanan sebagai bagian dari insiden keamanan;
ii. Mempelajari kerentanan baru dengan membaca sumber publik atau sumber pihak ketiga lainnya;

iii. Menemukan dan mencari kerentanan baru sebagai akibat dari aktivitas atau penelitian yang disengaja;
iv. Melakukan analisis tren dari *feed* dan data kerentanan dikumpulkan, untuk memahami konstituen atau TTP aktor serangan; dan
v. Membuat perencanaan, pengelolaan dan evaluasi kegiatan pada bagian teknis penelitian dan pelaporan kerentanan.

5.2.2. Fungsi Analisis Kerentanan

i. Melakukan pemindaian kerentanan secara berkala terhadap aset konstituen KBUMN-CSIRT;
ii. Melakukan pengumpulan, pengolahan dan analisis kerentanan keamanan siber lainnya yang mencakup ancaman, kerentanan dan produk/perangkat TI;
iii. Menyusun rekomendasi dari laporan kerentanan secara berkala;
iv. Melakukan reviu terhadap laporan kerentanan; dan
v. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan analisis kerentanan.

5.2.3. Fungsi Koordinasi dan Pengungkapan Kerentanan

i. Memastikan pemberitahuan informasi kerentanan tepat waktu dan terdistribusi yang akurat;
ii. Menjaga arus informasi dan melacak status aktivitas entitas yang ditugaskan atau diminta untuk berpartisipasi dalam merespons insiden keamanan informasi;
iii. Memastikan rekomendasi kerentanan dilaksanakan oleh konstituen KBUMN-CSIRT; dan
iv. Melakukan pengeolaan terhadap sistem elektronik yang digunakan dalam kegiatan koordinasi dan pengungkapan kerentanan.

5.2.4. Fungsi Respon dan Kerentanan

i. Memperbaiki atau memitigasi kerentanan yang ditemukan baik dari sistem monitoring dan pelaporan kerentanan untuk mencegah eksploitasi;
ii. Menerapkan *patch* atau solusi keamanan lain berdasarkan rencana tanggap insiden kerentanan dan *best practice*;
iii. Menyusun dan mendokumentasikan laporan respons kerentanan; dan
iv. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan respons kerentanan.

5.3. Layanan Pembinaan dan Publikasi

Layanan pembinaan dan publikasi menyelenggarakan fungsi yang terdiri dari:

5.3.1. Fungsi Berbagi Informasi

i. Membuat strategi komunikasi untuk membangun berbagi informasi keamanan siber;
ii. Mengelola akun media sosial terkait dengan publikasi KBUMN-CSIRT;
iii. Mengelola portal publikasi terkait dengan publikasi KBUMN-CSIRT;
iv. Memperhitungkan audiens pada saat informasi dibuat dan disebarluaskan;
v. Menerima masukan, laporan, komentar, dan pertanyaan dari konstituen KBUMN-CSIRT; dan
vi. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan berbagi informasi.

5.3.2. Fungsi Peningkatan Kesadaran Keamanan Siber

i. Membuat dan melaksanakan program edukasi keamanan siber;
ii. Membuat laporan publikasi mengenai kondisi terkini keamanan siber organisasi;
iii. Membuat publikasi teknis mengenai keamanan siber; dan
iv. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan peningkatan keamanan siber;

5.3.3. Fungsi Pelatihan Keamanan Siber

i. Membuat dan melaksanakan program pelatihan keamanan siber;
ii. Memberikan pelatihan dan pendidikan keamanan siber kepada konstituten KBUMN-CSIRT;
iii. Menilai, mengidentifikasi, dan mendokumentasikan kebutuhan kompetensi SDM untuk mengembangkan materi pelatihan dan pendidikan yang sesuai dan meningkatkan tingkat keterampilannya; dan
iv. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan pelatihan keamanan siber.

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 *screenshoot* 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.