

RFC 2350 SumedangKab-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 0.3 yang diterbitkan pada tanggal 24 April 2026

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.sumedangkab.go.id/file> (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditandatangani dengan sertifikat elektronik milik Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 SumedangKab-CSIRT

Versi : 0.4

Tanggal Publikasi : 13 Mei 2026

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Tanggap Insiden Siber - Computer Security Incident Response Team

Kabupaten Sumedang

Disingkat : SumedangKab-CSIRT

2.2. Alamat

Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang
Jalan Angkrek No. 103 Kelurahan Situ Kecamatan Sumedang Utara Kabupaten Sumedang, 45323

2.3. Zona Waktu

Kabupaten Sumedang (GMT+07:00)

2.4. Nomor Telepon

(0261) 201255

2.5. Nomor Fax

(0261) 201255

2.6. Telekomunikasi Lain

Tidak ada

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

csirt@sumedangkab.go.id

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

Bits : 4096

Key ID : 0x3141AABD9A1C241B

Fingerprint : EB9D 3152 1FB8 A921 01F8 BC60 3141 AABD 9A1C 241B

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

```
xsFNBGnwDcUBEADil8fXwqhR/jgLPzizUGfP3Qu8J0E81p2ug6bCAJp/iibvjNOD
C6Hs3nGbrjmPr2AQAOxCtDCX+/Mkr+5++kzVcdQeogIF7xrn2IJdu1SyugJx1IZ
Q/JargeXCXexTRfWoW5b+yzbNuSgUHV16ZkT6RoP+66BiPi+BWBROCMFDAhPt
JVp
uKSdbzn+4bAhxfeRRjlldmGgGHYpSOGmDQ8z3XIkYbV9DbCHZMAFjg8PTx5izCk
A
x7gNMDoGFI63rF1Rc7k24hIFwXa1lv0g9D6BeMit5synL0SjJLTfaqBipDOrUU6b
Zo6H7kiPXpSH9gaR8xjitOd7dyee6NBOFGuzsacPWBBPzsQsw9rQkHF27W7Y67C
X
04uRAKDHmCVYPInlCHyr6W05/YFBp1mVsXLtLFIqvndJhp0PbtiyPzpCFIY+keY
Tacu/xQ1mB4k+aSPEbMHag7f8SJ0LagrrGOOmNFIx16ZfXsnlcwz0rKKX+jM9Pnc
6p7mCbleYfC7WOD2N9qAybN9MgCfSfD4AvXRnHp3BKCEg8bAfIZ/nQv9wTLigd9
M
DvQbELHpw6ijW2DnG2J2/21nR0Rx8TYU1MvCxYTRzzFV19Q4aikFIEN0XqCw7F
FZ
a0f25dr4FZCUgpQzZ5hLIHnWaZ3o3eRHYKRm+jOqSxHGF3LuieUeJGLYjQARAQ
AB
zStTdW1lZGFuZ0thYi1DU0lSVCA8Y3NpcnRAC3VtZWRhbmduYWluZ28uaWQ+ws
GN
BBMBCAA3FiEE650xUh+4qSEB+LxgMUGqvZocJBsFamnWdCfYFCQWjmoACGw
MECwkl
BwUVCAkKCwUWAgMBAAAKCRAxQaq9mhwkGyp7D/sGss5/40NmBcmGskwkJI
MobR1Z
m2F4XpM9mgDuBwN/ZfnsqXuVApGre20n5r52MIgyRsUX+nX0j8XZGFLThEhzndtg
sbynQGVCgeRg+VExXUobitPPPzIG4EI0aTIJkC9cSoArD7rJXnQilB+C1V1tm+tg
JlpYHjGyRVsmN08Hhf6EuWkdHhMCYAgrdBOo7ejelDE8tS+/ov18N66LrDaQO9lx
```

K+NxWUzIVIADh1SeHjdbWLNGLBKAFnjcR3gHADekhmGsG45zccqMyYgjeVI0upXM
7lnhR6EOOh8iZjs1EsG0HSqUXhaJ9OQ/81/+5jnbObwcMSmJQ8VIARH7sE9a6r4l
/Vyv/DMJSIpNp4/vvQt0yF/tAAI6k94Rk0tp7NqEzOJli61VGB0x1uLYkjdhAGOV
IF7wjaP05PSiqoH+ynJsU2M95qewIRkmzTPalvEFI58bCdYgkf1GI34kHTo1Enu8
wloUTjezD3RN4zULNSw/D9HZNA13aWdHXzHCosfhSZ/WqQUUg8ZPvrPzSgTOX
Dyb
qcCStLpDlzU1+vMJFqmvf7nU3+NaU/LhOhCywCncR29vRWd518pXg6snd9ndsR/h
6Y9jBgJUKhhr0xxGIFUolgKgkot+7uyXsJ80e3e7iERR3QJlksWVpN660VTOBrqA
+c6/0vxMpwVN51imuM7BTQRp8A3HARAAzKDaQPR+WBTL5RtrXjMCwfKlj3D5fF
o4
DNQ9jBaPV98XHZbkCWeiybrlqt3/AHZblAc+AEvpr8Fws2CPXLBIOAa4hOIKhxdm
ME7Jsx6nRZdxjIN3YvSvQDI7ysRBc/p0eVtm22qTS6JLjD/8dsWuSEbl0Mbmfftt
gx3ahSNDUsIhFhD2AchFPgMY4krJCXT5Hq+uND5E3trmoMnhrZvOKJ6q+JJluMR
B
3+Bsg4nzOXbsolZeYoUxpUhcITi130yXIOv65HOKESJJWc3MOH70LWJGyj6Rzqz2
Xfz0xFllaALdV2BYSj44UhqFmSex9MP39F5SRb1k6vEEBfY/rQYI65aOmZGSvwy7
1H754pG7RhFH4BXfvegDNhnhSzxE/IKl8Tjkrxj65gi13wKHTqqRPT7/URnfvaBa
F6Ov2mvuh25fCzKHrQ6kQDcJIHtwq3GD6lpyGm2uoqDbhIG7KjzsFDJlInxxopFx
LLGOPqLjDdONZH5kG2ZQ4EhOJRoteWVcY/Gc7gQ2afs5eNaZ/6vNQv+Hk5MzD
khv
klQ51wMleWI3nZtk9vqgJJhPvGekhA5kcFYLBqgkcNpnv0qz2eeKoz0cPQBusav4
AlpgMrnC0Kraic7Fbi4ZDUbm2tx8agNoh0qjm4wu/GI9iK33rFhh5HOO46qosXQU
ZQxAsxm4F3sAEQEAAcLBfAQYAQgAJhYhBOudMVIfuKkhAfi8YDFBqr2aHCQbB
QJp
8A3HBQkFo5qAAhsMAAoJEDFBqr2aHCQbhtQP/3i54yuUHg9nTzrAa6Kh+XesCE7
+
uNGHF+iqtELT1baNfLSsskJBZVv5uh1vZTzPNmDdM0AmCXJMp+t0i/AcihrcLtz
VeRgn5k/neGR9JMkgFnRDHsx1DaHwUfpoi1NjdJtztTinXIZNwt1kL2SmA+1a7Z
gqVOJRDci+ce/zCXa7xQBNUQ59NWUsQa+yRR+ZnwotSsh6lIHlusyRgvJe/pqr14
p49rKvBUImrNKnKd5s/K36qvd9lx4eT1XXglD7tCppKcYr5zujq0bU6+zd46MBAH
iHwh75HECiVtNaMAAtQ8h7eMH6GCBCvMd855wtZknZ693wARR97RTN8Ctay1Pf
r8
j3gN0+SO0d7UXW7i3ew2oP7sqku+drn4/BYPUPXmTm2RouowHNGUr9eEDUKrS
2g3
Kp/wE1yvRivxsAsLgM/8fpjfDlc8T2fyJ9zQ2m8vgv8T7f78r7dI9XT0nzKHEYX+
G6qvgKJezLH2Fngp7jSPa6Q2lhBFAOa+8qAhwj83onZJKVV2bE/44TR2K9wqELry
k4AzuURK574lw9ZnMgLWIMTywFcq7iztoWq/c3B9z0V1CktoZOChIYyU0c2kxRDs
uSplXDXDo4zXgTQzf/YWFhQkK5A+QJDbBqJ9SZDdkYUR0Cv3EW3zeH14ETHLju
x6
bzw6RdUrY2zXUaBp
=26Rg
-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada :

https://csirt.sumedangkab.go.id/storage/public-key/SumedangKab-CSIRT_csirt@sumedangkab.go.id-0x3141AABD9A1C241B-pub.asc

2.9. Anggota Tim

Pengarah CSIRT adalah Sekretaris Daerah Pemerintah Kabupaten Sumedang, penanggung jawab CSIRT adalah Asisten Perekonomian dan Pembangunan Kabupaten Sumedang, Ketua SumedangKab-CSIRT adalah Kepala Dinas Komunikasi, Informatika dan Statistik Kabupaten Sumedang, Sekretaris CSIRT adalah Sekretaris Dinas Komunikasi, Informatika dan Statistik Kabupaten Sumedang, dan anggotanya dari Pegawai yang menangani insiden siber / teknologi informasi di masing-masing Satuan Kerja Perangkat Daerah di Pemerintah Kabupaten Sumedang.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak SumedangKab-CSIRT

Metode yang disarankan untuk menghubungi SumedangKab-CSIRT adalah melalui *e-mail* pada alamat csirt@sumedangkab.go.id atau melalui nomor telepon (0261) 201255 pada hari kerja jam 08.00 - 15.30 (Senin-Kamis) dan 08.00 - 16.00 (Jumat).

3. Mengenai SumedangKab-CSIRT

3.1. Visi

Terwujudnya sistem elektronik yang andal dan aman di lingkungan Pemerintah Kabupaten Sumedang, dengan penerapan prinsip keamanan informasi serta kemampuan penanggulangan dan pemulihan insiden siber yang efektif..

3.2. Misi

Misi dari SumedangKab-CSIRT, yaitu :

- a. Membangun pusat pencatatan, pelaporan, penanggulangan dan pemulihan insiden siber di lingkungan Pemerintah Kabupaten Sumedang;
- b. Menyelenggarakan penanggulangan dan pemulihan insiden siber melalui kegiatan mendeteksi, menganalisis, mitigasi, pemulihan dan melakukan upaya pencegahan terhadap insiden siber
- c. Membangun skema kerja dalam penanggulangan dan pemulihan dengan melakukan koordinasi dan kerja sama dalam rangka mencegah dan/atau mengurangi dampak dari Insiden Siber pada konstituen;
- d. Membangun kapasitas sumber daya keamanan siber pada sektor Pemerintah Kabupaten Sumedang; dan
- e. Meningkatkan kesadaran pentingnya keamanan informasi bagi sumber daya manusia di lingkungan Pemerintah Kabupaten Sumedang..

3.3. Konstituen

Konstituen SumedangKab-CSIRT meliputi Satuan Kerja Perangkat Daerah penyelenggara sistem elektronik di lingkungan Pemerintah Kabupaten Sumedang

3.4. Sponsorship dan/atau Afiliasi

Pendanaan SumedangKab-CSIRT bersumber dari Anggaran Pendapatan dan Belanja Daerah (APBD).

3.5. Otoritas

SumedangKab-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden siber di lingkungan Pemerintah Kabupaten Sumedang.

SumedangKab-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya namun tidak berkaitan persoalan hukum, dan dapat berkoordinasi serta bekerjasama dengan BSSN/ Akademisi bidang IT Security/ Tenaga Ahli Security/ pihak lain untuk insiden yang tidak dapat ditangani

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

SumedangKab-CSIRT melayani penanganan insiden siber dengan jenis berikut :

- a. *Web defacement*
- b. *DDOS (Distributed Denial of Service)*
- c. *Phising*

Dukungan yang diberikan oleh SumedangKab-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis, dampak insiden dan layanan yang digunakan.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

SumedangKab-CSIRT akan melakukan kerjasama dan berbagi informasi dengan JabarProv-CSIRT, BSSN selaku Gov-CSIRT dan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh SumedangKab-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, SumedangKab-CSIRT dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional), telepon atau fax. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

5. Layanan dan Fungsi

5.1. Layanan

Layanan dari SumedangKab-CSIRT yaitu :

5.1.1. Layanan Utama

Layanan Utama merupakan layanan reaktif SumedangKab-CSIRT yang terdiri dari :

5.1.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan pemberian peringatan keamanan siber adalah layanan yang memantau, mendeteksi, dan menyebarkan informasi mengenai ancaman

atau kerentanan siber kepada pihak yang berkepentingan agar dapat mengambil tindakan pencegahan atau respons yang tepat waktu.

5.1.1.2. Penanganan Insiden Siber

CSIRT memiliki peran penting dalam melakukan penanganan insiden siber dengan melakukan kegiatan mendeteksi, merespons, dan mengatasi insiden keamanan siber. Berikut adalah beberapa layanan dalam konteks penanganan insiden siber:

- a. deteksi insiden: mendeteksi aktivitas mencurigakan atau tanda-tanda insiden keamanan siber.
- b. analisis insiden: menganalisis insiden untuk memahami asal usul, dampak, dan metode serangan.
- c. mitigasi dan penanggulangan: mengambil tindakan cepat untuk mengurangi dampak insiden dan menghentikan serangan.
- d. pemulihan: membantu organisasi dalam pemulihan operasi normal setelah insiden.
- e. analisis forensik: menyelidiki asal usul insiden dan mengumpulkan bukti forensik jika diperlukan.
- f. rekomendasi pencegahan: memberikan saran untuk mencegah insiden serupa di masa depan.

5.1.2. Layanan Tambahan

5.1.2.1. Layanan Reaktif

Layanan reaktif mencakup serangkaian tindakan tanggap cepat dalam menghadapi ancaman dan gangguan digital, meliputi penanganan kerawanan Sistem Elektronik yakni proses identifikasi, analisis, dan mitigasi celah keamanan yang ditemukan pada infrastruktur atau aplikasi yang berpotensi dieksploitasi oleh pihak yang tidak bertanggung jawab serta penanganan artefak, yaitu kegiatan pengumpulan, pemeriksaan, dan analisis bukti digital atau komponen berbahaya yang ditemukan sebagai hasil dari suatu insiden siber, guna mendukung proses investigasi dan pemulihan sistem secara menyeluruh.

5.1.2.2. Layanan Proaktif

Layanan proaktif, yang merupakan upaya antisipatif dan pencegahan dini sebelum terjadinya insiden keamanan siber, meliputi pemberitahuan hasil pengamatan terkait dengan berbagai ancaman yang berpotensi muncul akibat perkembangan teknologi seperti munculnya teknik serangan baru, kerentanan pada perangkat lunak terkini, maupun evolusi metode eksploitasi yang semakin canggih. Perkembangan politik yang termasuk ketegangan geopolitik yang dapat memicu aktivitas peretasan bermotif

ideologis atau serangan siber yang disponsori negara serta perkembangan ekonomi seperti meningkatnya kejahatan siber berbasis finansial yang memanfaatkan kondisi pasar atau krisis ekonomi tertentu sekaligus mencakup kegiatan pendeteksian serangan secara real-time, yaitu pemantauan berkelanjutan terhadap lalu lintas data dan aktivitas sistem guna mengidentifikasi indikasi awal serangan sebelum dampaknya meluas dan merugikan lebih jauh.

5.1.2.3. Layanan peningkatan kesiapan penanganan siber

Layanan peningkatan kesiapan penanganan siber bertujuan untuk memperkuat fondasi keamanan organisasi secara menyeluruh sehingga mampu menghadapi ancaman siber dengan lebih terstruktur dan terukur, meliputi analisa risiko yakni proses sistematis dalam mengidentifikasi, mengevaluasi, dan memprioritaskan potensi ancaman serta kelemahan yang ada pada infrastruktur, sistem, maupun proses organisasi, sehingga dapat diambil langkah-langkah penanganan yang tepat dan proporsional sesuai dengan tingkat risiko yang dihadapi.

Konsultasi terkait kesiapan penanganan insiden siber yaitu pemberian asistensi teknis dan strategis kepada organisasi dalam merancang, menyusun, serta mengevaluasi prosedur dan kebijakan tanggap insiden, termasuk di antaranya penyusunan *incident response plan*, pembentukan tim tanggap insiden, serta pelaksanaan simulasi atau *tabletop exercise* guna mengukur kesiapan organisasi dalam menghadapi skenario serangan nyata serta pembangunan kesadaran dan kepedulian terhadap keamanan siber, yaitu serangkaian upaya edukasi, sosialisasi, dan pelatihan yang ditujukan kepada seluruh elemen organisasi, mulai dari pimpinan hingga staf operasional, agar setiap individu memahami peran dan tanggung jawabnya dalam menjaga keamanan informasi serta mampu mengenali dan merespons ancaman siber sejak dini.

5.2. Fungsi

5.2.1. Fungsi Utama atas layanan SumedangKab-CSIRT

- 5.2.1.1. pemberian peringatan terkait Keamanan Siber;
- 5.2.1.2. perumusan panduan teknis penanganan Insiden Siber;
- 5.2.1.3. pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;
- 5.2.1.4. pemilahan (triage) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani;

- 5.2.1.5. penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan; dan
- 5.2.1.6. diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.

5.2.2. Fungsi Lain atas layanan SumedangKab-CSIRT

5.2.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan berupa koordinasi, analisis dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*). 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 berupa tindak lanjut atas kegiatan *Vulnerability Assessment*.

5.2.2.2. Penanganan Artefak Digital

Layanan ini diberikan berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi.

5.2.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan berupa pemberitahuan hasil pengamatan potensi ancaman dan sistem deteksi yang dilakukan mandiri maupun dari BSSN. SumedangKab-CSIRT memberikan informasi kepada penyelenggara sistem elektronik terkait layanan ini.

5.2.2.4. Pendeteksian Serangan

Layanan ini berupa identifikasi kerentanan, penilaian risiko atas kerentanan, serta hasil dari perangkat pendeteksi serangan yang ditemukan. SumedangKab-CSIRT memberikan informasi terkait layanan ini.

5.2.2.5. Analisis Risiko Keamanan Siber

Layanan ini berupa analisis risiko keamanan siber. SumedangKab-CSIRT memberikan informasi terkait layanan ini

5.2.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini diberikan SumedangKab-CSIRT berupa konsultasi terkait prosedur, metode dan teknis penanganan insiden siber dalam upaya penanggulangan dan pemulihan insiden.

5.2.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

SumedangKab-CSIRT melaksanakan, mendokumentasikan, dan mempublikasikan kegiatan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@sumedangkab.go.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

7. Disclaimer

- a. SumedangKab-CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada Satuan Kerja Perangkat Daerah di Lingkungan Pemerintah Kabupaten Sumedang;
- b. Terkait penanganan insiden siber tergantung dari ketersediaan *tools* yang dimiliki;
- c. Setiap tindak pencegahan akan diambil dalam penyusunan informasi, pemberitahuan dan peringatan, maka SumedangKab-CSIRT tidak bertanggung jawab atas kesalahan dan kelalaian atau kerusakan yang diakibatkan dari penggunaan informasi yang terkandung dalamnya. SumedangKab-CSIRT juga tidak memiliki wewenang dalam persoalan hukum.

Sumedang, 13 Mei 2026

