

RFC 2350 SANGGAUKAB-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 5 November 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Seluruh Perangkat Daerah di lingkungan Pemerintah Kabupaten Sanggau.

1.3. Lokasi dimana Dokumen ini bisa didapat

<https://csirt.sanggau.go.id/rfc2350/indonesia.pdf>

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP Key milik SanggauKab-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 SanggauKab-CSIRT;

Versi : 1.0;

Tanggal Publikasi : 5 November 2024;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team Pemerintah Kabupaten Sanggau
Disingkat : SanggauKab-CSIRT.

2.2. Alamat

Jalan Jenderal Sudirman Nomor 10, Kel. Beringin, Kec. Kapuas, Kab. Sanggau,
Kalimantan Barat, 78512

2.3. Zona Waktu

Kota Sanggau (GMT+07:00)

2.4. Nomor Telepon

(+62) 5642020984

2.5. Nomor Fax

(+62) 5642020984

2.6. Telekomunikasi Lain

<https://diskominfo@mail.sanggau.go.id>

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

csirt@mail.sanggau.go.id

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

Bits : 4096

ID : F1935672

Key Fingerprint : 1C58 B155 D934 9713 D51D 2753 AD68 26F7 F193 5672

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

mQINBGcMhnUBEAC7wMBnA1YwSU0yLxqtUtGjFWIUIOmLg0jVB0fdv6cnUZoVheB
ajjMwxwRR9XIN90HgwLlzb0YUlcZ5knBxppCoEtaBQzrgAQVraP1ChS0DySU2y9A
7G1MAnAA0ZlZjjEv1DSyB4YlhsbsUcTiUFIZeGyvoQV6qrXR6uFbymwnCbaA5A3Y
gwmweal4yJfww/hKNd58OEwNHPHEXx7MiTqPnsi0hSLvZhFTho07XB2xsbCCKy6j
px7E4lxtHndRpvqdWqAOOrChXjN/vRMXalwi1luvl9V8ued2a+RmpFqSFXtee8IS4
ZMyEndiNBc9HITssrFGY8s8kypkBl2p7wwwOFo11Nej8ttDOiGpjDDR5t2CfHq0O
bcWABUA9j0EDFP4Ey6RJP0RLpMtuPvgBKgqz+mpC6c0D+aSs0ES+w+xWQ/BGRRuj
dnS3Tu7pZaUXtrRiDI0UGuGvk9rzaasZecfEhur8j9NH/S/ZK4yvkbIC8TGJzXW
7RQ73oeWR3WKhmL6blmwGpLWtVdaBZrSOZjKG/vwaQ93GNtS+JgpHQZu27a0f2i
1tj6UK7hgSaD2YPF0aA4OQ0n7NXqM1HKzOndhn1O7lg0A3mtx7bXTjPVrH+j+UOF
XWjk7HzNNNoPO9I7o7k34sSD+bH3S+oAZePRixiUs3M4IQxCKma82XfXAgwARAQAB
tCtTYW5nZ2F1S2FiLUNTSVJUIDxjc2lydEBtYWlsLnNhbmduYXUuZ28uaWQ+iQJO
BBMBCAA4FiEEHFixVdk0lxPVHSDTrWgm9/GTVnlFAmcMhnUCGwMFCwkIBwIGFQoJ
CAsCBBCAwEChgECF4AACgkQrWgm9/GTVnl9IRAAtroQrArNxxB8CrBmqLC4DV/5
l+URO9FTftroaJ+OrkkoCgVYOB9NXloTzjeYlaWvVzn9B9H2Xk4Yhb5LSRyxa8Bo
Nskfh78Atgq088HAcjOsRePcvjNsMnfkvrNcyXmUdRCeJMYcrs25CubY06qaATmW
AanOK2M2WrsxuMV9Ktu6HewWY2eHk701Z60VSdjC+BT0CP1NDqY06gclR/eyiMpV
4M7eJO/gumjp9GhWv81w8efma7pYzLB2gNDuyUMVxEbAEQ8vTXgdOITKutB+X4W
Ac56ghrCMTGoKTVQS0EA05F0jzGpXmU2BKEKszDJOqXMc4yO0KRx5TSzTglxmDY/
bXmvmIX9LD/xKh28qGDFoMMAR4YXtOyBRZZ/01wEEle4tM1+UdJGtal5gfobrRev
HjForglBHGM2DkppzsJ3BHo7aGz5aU/YD/fKiR7cNJIftI0b6eInzEaAxSU1aZqC
DkLHVJaRemAiaGlxbOe2VnIKTY8isnRWby6BSiRfDjaFkiUIHGxOTNdv9Oze09FW
lQugM582NnNzQJjg4JTYoOKUiBL0DvSHLG4jH6ToHFPJn7df+lKRCZI1Pt3FoOD
3oU8ZPyjwzVNx4QWTrc9zd6cG9ZSvUciWmD3vyCaeXUts8/UBTfyCri477rDhyZP
qKWZeDZr5VBq46HmV4y5Ag0EZwyGdQEALnjVlkyW/uCPSFSduTiiaNjm/zUVRO
tGosbChi6wP3llustbiSo/n8Fa/5QqidmwY3W+KHDS5VvtDDTQN6xBBT6nulrn/0
EdvVQPTTto4uWm8dthv8MG6+fKZXaid7jWvyl4kNJBuOveMsduI4EA07KMmXWd4Y
82nfi9sZiGfEdu2asMGUw9aOMARRI9pBw8a/jSlbnxU4Ooo3hUuAgMnM1tPo3DtL
bRuLHo7/e/GNfwcyTaC/PSFPRJL5gFzOP7Z+CUW+2TSEzbaX8JcB76Wphreu63SY
cmzs2SuXTr216Ej9FjTa7Nu9BelHS7SdpRL5r48J/8wZi5FD/m0IYXI/BiAMYMXO
PMh3TXkX0ew8Xb1dmQj2C5NikTH6vHSusq8d2IU6lchGyyEfTWWhp7atdMZwukr8v
lpy9LLL1pG62a26hY6NlcltiqrtX1ehKvinNmj/R6NuhzsiFktmhjggXoSd1MKgV
B4rUoBd2W6nid+OpGoas2n4eODgSIsaA4Iaoq7QXPb3Ca83p5rijbe/UfvPjUv/8
Lolchvue4CYSQydK3F4hDQns3v0B4oTra4OPW0eF98HLjPTEfAR5cfNFPgE7s9Bw
wFiv9+btI8jybJSid7C+FHCZfKuXW9aQin8c6TcowQgP4ux4+adj7ZgQ5nQCyWws
ONByTt2+FmxadABEBAAGJAjYEGAEIACAWIQQCWLFV2TSXE9UdJ1OtaCb38ZNWcgUC

ZwyGdQIbDAAKCRCtaCb38ZNWcvhHD/4k6zd92rU110v+QwE6hmQib2G1Bct78qkg
ASWA2ya9LYH3naBvgO92P3lzCacZENiWVWhPuNUgY4s2lhE9On6agbS0jtCMPY20
ZMWU3g1+b8zi6OHl1SXVmKnIDuQa5q2j4w2kMrlwAn415Dgi+S6MtFVER8R9/Agt
QXaZTjboNbZyrFvGabzqnnF/vV8mVQ4sWNNqAwovN3Gy/RPmlJMM6ntsdiUzyzgp
j7/nCkt4fkPoUaPEYfIXcV8iBZC7Nu6v4D3AvwA1bsSqkleNV3D/CsECRhtbArSR
5wsvJ7ToBewOY9A7iAgiUcrem3FAg3umGsVQKhBrU3ut2LoDKTojcxE58zumtNsb
Q6oa0pmUaMIRw9gu4X/+iL0YwwJjySAZSa/o6kXkrnDG+IBj4/VPXE7+gbWY3adm
oh4J7Bz+E9sAZ7tyUZqAsSgErzziy7GMooa2VF3FNid0NWBHj5fsu522ToUcnsGa
HRougDKlw7dfAYXctNw40oAHviSn3UvzW0yfCcNcB/XloUzFQ+f7+EMiDN4V43+w
NDJMzTohl1Okvnb8hm0ZEG9FUPKOENO0YFWYf01qZT2wCyGo0xoOrpkudnfvPaNU
jLXJuByRUBO+B8ORSIhTMC5VIVvSXuLIY/eMyBGHKV4JBW6AuKAfkDUKj57rPP3B
taOVI//1ZQ==

=ej6D

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

File PGP key ini tersedia pada :

<https://csirt.sanggau.go.id/publickey.asc>

2.9. Anggota Tim

Penanggung jawab SanggauKab-CSIRT adalah Sekretaris Daerah Kabupaten Sanggau, Ketua SanggauKab-CSIRT adalah Kepala Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Sanggau, Sekretaris SanggauKab-CSIRT adalah Sekretaris DISKOMINFO Kabupaten Sanggau, Ketua Tim Penanggulangan dan Pemulihan Insiden adalah Kepala Bidang Statistik dan Persandian, Wakil ketua Tim Penanggulangan dan Pemulihan Insiden Kepala Bidang Pengelolaan Pemerintahan Berbasis Elektronik DISKOMINFO Kabupaten Sanggau, Ketua Sub Tim Pengelola Jaringan dan Server adalah Pejabat Fungsional Ahli Muda pada Bidang Pengelolaan Pemerintahan Berbasis Elektronik DISKOMINFO Kabupaten Sanggau, Ketua Sub Tim Keamanan Informasi adalah Pejabat Fungsional Ahli Muda pada Bidang Statistik dan Persandian, Ketua Sub Tim *Website Administrator* dan Aplikasi adalah Pejabat Fungsional Ahli Muda pada Bidang Pengelolaan Pemerintahan Berbasis Elektronik DISKOMINFO Kabupaten Sanggau, Ketua Sub Tim Agen CSIRT adalah Kepala Perangkat Daerah di lingkungan Pemerintah Kabupaten Sanggau.

Yang termasuk anggota tim adalah seluruh staf pelaksana dan fungsional di lingkungan Dinas Komunikasi dan Informatika kabupaten Sanggau serta pengelola TIK pada masing-masing Perangkat Daerah di lingkungan Pemerintah Kabupaten Sanggau

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak SanggauKab-CSIRT

Metode yang disarankan untuk menghubungi SanggauKab-CSIRT adalah melalui e-mail pada alamat <https://csirt@mail.sanggau.go.id> atau melalui nomor telepon (0564) 2020984 ke Tim SanggauKab-CSIRT pada hari kerja selama pukul 08.30 – 14.00 WIB.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi SanggauKab-CSIRT adalah terwujudnya keamanan siber yang tangguh dan terpercaya pada sistem pemerintahan berbasis elektronik untuk terselenggaranya birokrasi dan pelayanan publik yang prima di lingkungan Pemerintah Kabupaten Sanggau.

3.2. Misi

Misi dari SanggauKab-CSIRT, yaitu:

- a. Mengkoordinasikan penanganan insiden keamanan siber di lingkungan Pemerintah Kabupaten Sanggau.
- b. Menjadi pusat pelaporan, serta penanganan insiden keamanan informasi di lingkungan Pemerintah Kabupaten Sanggau.
- c. Membangun dan mengembangkan kapasitas sumber daya keamanan siber di lingkungan Pemerintah Kabupaten Sanggau.

3.3. Konstituen

Konstituen SanggauKab-CSIRT meliputi seluruh pengguna sistem elektronik di lingkungan Pemerintah Kabupaten Sanggau.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan SanggauKab-CSIRT bersumber dari APBD Pemerintah Kabupaten Sanggau.

3.5. Otoritas

SanggauKab-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Pemerintah Kabupaten Sanggau. SanggauKab-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya dan dapat berkoordinasi serta bekerjasama dengan Gov-CSIRT, BSSN, maupun Konsultan Keamanan Siber untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

SanggauKab-CSIRT melayani penanganan insiden siber dengan jenis berikut:

- a. *DDos*;
- b. *Web Defacement*;
- c. *Malware*;
- d. *Phising*;
- e. *Spamming*;
- f. *Social Engineering*;
- g. *Network Incident*;

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

4.2. Kerja Sama, Interaksi dan Pengungkapan Informasi/Data

- a. SanggauKab-CSIRT akan melakukan kerjasama dan berbagi informasi dengan Gov-CSIRT atau CSIRT lainnya atau organisasi lainnya dalam lingkup keamanan siber;

- b. Seluruh informasi yang diterima oleh SanggauKab-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, SanggauKab-CSIRT menggunakan alamat e-mail dinas tanpa enkripsi data (email konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat melalui email dinas dengan menggunakan enkripsi kunci publik menggunakan PGP.

5. Layanan

5.1. Layanan Utama

Layanan utama dari SanggauKab-CSIRT yaitu:

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan.

5.1.2. Layanan Penaggulangan dan Pemulihan Insiden

Layanan ini berupa koordinasi, analisis, rekomendasi teknis dan bantuan *on-site* dalam rangka penaggulangan dan pemulihan insiden siber.

5.1.3. Layanan Penanganan Kerawanan

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

5.1.4. Layanan Penanganan Artifak

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

5.2. Layanan Proaktif

Layanan proaktif dari SanggauKab-CSIRT yaitu:

5.2.1. Layanan Security Assessment

Layanan ini berupa analisis sistem keamanan untuk mengidentifikasi kerentanan dan kelemahan sebuah sistem elektronik sehingga dapat memitigasi resiko insiden.

5.2.2. Layanan Security Audit

Layanan ini berupa identifikasi dan evaluasi terhadap kebijakan, prosedur dan kontrol keamanan untuk memastikan bahwa sistem keamanan yang ada telah diimplementasikan dengan benar dan efektif sesuai dengan standar yang ditentukan.

5.3. Layanan Manajemen Kualitas Keamanan

Layanan manajemen kualitas keamanan dari SanggauKab-CSIRT yaitu:

5.3.1. Layanan Analisis Resiko

Layanan ini berupa identifikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan.

5.3.2. Layanan Edukasi dan Pelatihan

Layanan ini berupa kegiatan literasi keamanan informasi seperti *workshop*, seminar dan sosialisasi serta kegiatan peningkatan kapasitas sumber daya keamanan informasi seperti bimbingan teknis, pendidikan dan pelatihan keamanan informasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke [csirt\[at\]mail\[dot\]sanggau\[dot\]go\[dot\]id](mailto:csirt@mail.sanggau.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

Untuk penanggulangan *malware* tergantung dengan *tools* yang dimiliki.