RFC 2350 SIAK CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 1 Oktober 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.siakkab.go.id/document/rfc-2350-siak-csirt-versi-bahasa-indonesia (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen ini ditandatangani digital menggunakan sertifikat digital BSSN oleh Kepala Dinas Komunikasi dan Informatika Kabupaten Siak.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 SIAK-CSIRT;
Versi : 1.0;
Tanggal Publikasi : 1 Oktober 2025;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

Kabupaten Siak - Computer Security Incident Response Team (CSIRT)
Disingkat : SIAK-CSIRT.

2.2. Alamat

Kompleks Perkantoan Tj Agung, Kabupaten Siak

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

0821-7031-8910

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

-

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

csirt@mail.siakkab.go.id

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

Bits : 3072
ID : 0x41E37B66A8E090CD
Key Fingerprint : CBCC 3A84 451F 0990 04EF BB29 41E3 7B66 A8E0 90CD

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

xsDNBGiS1fABDADHPTdeT4XqP+9gfVAzxA4mROKUpPHqn5dGX0RarPQurqaOE
giKs+v2X0gaTS7PbW2MBd/1Q76eRg7lg2eA0QKikAZqlFcD3aq8St3FpN/CAUFRm
w0wdIbVA0LVBb7w8wXQxopOOSXbIWxXryvJPt9l8yUFyIE42Ybmjak/KCCO3N0v1
Mx/7i1uzfKJ6XXjNBt2PHCuUVg/CZzWA6i2D40CmEwSyAHTEuSynvYQBGG07OS
F0vEQYASePbXoqutvfX/allw0q6r4CkEO696PaFvSAHIz73EbUDKAQaTN8R/tWgcF
z/ZSXwSRMfP+HOILDuvmr0Jp6x+zNsGWUXLhPw8nOyYtj4Mq8XupkHMNNspBTs
Bp6s9M1TG+jnh/GBFAJEp4iBc9lodEPKFBHOYaslqht4bjG4IIXrwGihdQsfFznX6q9
39MiyOp+UAWA2k3xO4U34RDL58gS+Q23qoiRCHceynT2DXQ0GTY9Ywmj5tTk4
X3/lWzBZXyJ5G6ZcaiJV0AEQEAAc0lU0lBSyBDU0lSVCA8Y3NpcnRAbWFpbC5za
WFra2FiLmdvLmlkPsLBDQQTAQgANxYhBMvMOoRFHwmQBO+7KUHje2ao4JDN
BQJoktXwBQkFo5qAAhsDBAsJCAcFFQgJCgsFFgIDAQAACgkQQeN7ZqjgkM0nb
AwAsOzrDn9+jAs11qn26cZBBdVpmnhxgW1YMEHwIBczHbP9bdx8hcrE9LeRscK8
FebCrClMUIAT9BGzrRQSt6OKMSlSgvw2vidtao/ozz9TBq8zaqbKN469rs7QrgCZYc
QQbK3j5Sp8Ze0KJXNoLKrQGdwUbD7qk+c6fMlGfltO3aQypxbZYl2ZwvCgbkvZPM
YyDhqFqq0cqbp8BcuW/J26QFtwLVaMDOamSW/AKoQ+Dohtvr7u2QkN6F9EkqvG
UnwqIo4Kt6otEjzF4R3ZsIW5rRP47XIVzl2Wt+C2gY2yFG2xJvIjtmIpzU9xQEV62JfT
1mkq6YkwFsxB1vfRdJnR8VttSwvLRFqXWEENIkIJdzsR/RGmWK71W7YxTd41rR
OLOMgKewd96GtxkoKoufAllTI+qFXQDPr0FRCVr5oKfRmwRusqeRYKiwM2lzUOie
EjryCEfJF4omvF2gJ49OLK73zLY+DVLIP2MGAaHaA8Ve/BW0yNHHc01ta7eRiKaI
3kzsDNBGiS1fEBDADsnaHbFiU9238BnKxCfStUbPxIc2F6Hi9TPFXnedMJgFiWmpI
+0pKXH7im5bDLUKrUtvxBwICJg655DrkmfMZSs1a6xMlzrUf/EqD9i9mWIHcirUeqX
xdUvI4YNbkNseukNiQyWdeKmHrRlIhKDSTAl6MqwyZ0OxGRt4t3WPx3ZNFWhFy
H+tWZCWFacvsyd8JCLaMK29zaWZwhF2nTV2Fo0BD8gE+lwLTG20/v6y7HRTSO
2BChQOTXROdF94ZtK/dflDxbW3WR8yKwDxQN1fQjvl+8G3AQ6WfdsHg6OWuYb
U/zVE2ogrkemW62FyDa82/MPJpdJyYMO17Zmiu4b3bVdahzx7aE55CBcSvAepdU
av30ws6qvNtwNOSW1P3qB7SnkRSQgkLFAwfwQXOve9H/xnw6wL7EXIO0akcfcE
Dyxr7lsglAuGTAOBtduQyETIL92Qnz1AxPDQ5FMGK7qgUUkK+U6MeFqTLh1mYn
pZYH1EDwaenWAokmxrY21cTVoDEAEQEAAcLA/AQYAQgAJhYhBMvMOoRFHw
mQBO+7KUHje2ao4JDNBQJoktXxBQkFo5qAAhsMAAoJEEHje2ao4JDNmPIL/0jVy

RUMVtvGgWImIGL5p6KG1zsJPyjpScYJgqfrdi51sX6LZRFiZ4HXMxACc8GgRCJf4
ouD1Tjyl1ze7vR+qbEjDO1Xlmf75C+ZZHrUiUqnR7gdhO4K+vAPIHVcqSYR92rBd0
MPJX+RnlBMXcJ+JaL1yow3w44ic1PkDcSuxUB4XASTOC6ceNlZ3UXI/ompPJu2x
RqojlAbxX95m2KmQzcWGWG4SAMXAayoSvtwCZwjsh4Jrub39ViFw64iSVaK6aZi
+xIB9jjD29JazSA/KASy2y7aVty9WIvLbSR/N9G7wZnQECRKGV2rZAkZQS6CcX8U
qcG3/tUG0lIBIwfLL4wQH9pH0uJnkPZ5oDheCocluX3jhFHwrJY5gdhJwFHKQ8hQ0
vT3l5gKth+jYbplzFgHvfAuthHUmcNqoPn8KxSCnYZzNSWbp+NQmfV6Foc0aONA/
/L+pkZpeUZvT61dpYfcFhKZ7rj/S0qN0UXkvxEf488b1r1vZa5gu7iRwceUbA===jC6c
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.siakkab.go.id/SIAK-CSIRT-public.asc

2.9. Anggota Tim

Ketua Siak-CSIRT adalah Kepala Dinas Komunikasi dan Informatika Kabupaten Siak. Sekretaris Siak-CSIRT adalah Kepala Bidang Teknologi Informasi Komunikasi dan Persandian dan Ketua Tim Penanggulangan dan Pemulihan Insiden adalah Amarullah Aman, S.Kom., M.Si. Terdapat 4 Sub Tim yaitu :

1. Tim Pengelola Jaringan dan Server
2. Tim Manajemen Keamanan Informasi
3. Tim Pengelola Website Administrator dan Aplikasi
4. Sub Tim Penerima Laporan Insiden Siber

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada kontak SIAK-CSIRT

Metode yang disarankan untuk menghubungi SIAK-CSIRT adalah melalui *e-mail* pada alamat csirt@mail.siakkab.go.id pada hari kerja.

3. Mengenai SIAK-CSIRT

3.1. Visi

Visi Siak-CSIRT adalah Terwujudnya ketahanan dan respons insiden keamanan siber yang tangguh, adaptif dan terpercaya di Lingkungan Pemerintah Kabupaten Siak guna mendukung tata kelola pemerintahan digital yang aman dan berdaya saing.

3.2. Misi

Misi dari SIAK-CSIRT, yaitu :

a. Mengembangkan sistem deteksi dini, respons cepat, dan pemulihan insiden siber secara terpadu dan berkelanjutan untuk menjaga ketersediaan, keutuhan dan kerahasiaan informasi pemerintah daerah.

b. Meningkatkan koordinasi dan kolaborasi lintas perangkat daerah dan dengan lembaga terkait di tingkat pusat maupun daerah, termasuk BSSN dalam menangani insiber siber secara terstrandar dan profesional.
c. Membangun kesadaran dan budaya keamanan siber melalui edukasi, pelatihan dan simulasi secara berkala kepada ASN dan seluruh pemangku kepentingan di Lingkungan Pemerintah Kabupaten Siak.
d. Meningkatkan kapasitas dan kapabilitas teknis sumber daya manusia di bidang keamanan informasi dan siber, selaras dengan kerangka kerja nasional keamanan siber (*National Cybersecurity Framework*).
e. Mengintegrasikan kebijakan dan prosedur pengamanan informasi dengan arsitektur SPBE dan infrastruktur TIK Pemerintah Kabupaten Siak sesuai dengan regulasi nasional yang berlaku.

3.3. Konstituen

Konstituen SIAK-CSIRT meliputi :
a. Bupati Siak
b. Wakil Bupati Siak
c. Sekretaris Daerah Kabupaten Siak
d. Pimpinan OPD di Lingkungan Pemerintah Kabupaten Siak

3.4. Sponsorship dan/atau Afiliasi

Pendanaan SIAK-CSIRT bersumber dari APBD Kabupaten Siak.

3.5. Otoritas

1. Mengakses sistem dan data terkait insiden
   SIAK- CSIRT memiliki kewenangan untuk mengakses sistem, log, dan data yang relevan guna melakukan analisis insiden keamanan siber secara menyeluruh.
2. Melakukan investigasi dan analisis
   SIAK- CSIRTberwenang melakukan investigasi atas insiden, termasuk mengumpulkan bukti digital, menganalisis dampak dan mengidentifikasi penyebab utama insiden siber.
3. Koordinasi dengan pihak internal dan eksternal
   SIAK- CSIRT memiliki otoritas untuk berkoordinasi dengan unit kerja terkait di dalam organisasi maupun dengan pihak eksternal seperti BSSN, penyedia layanan internet dan lembaga hukum apalagi diperlukan.
4. Mengambil tindakan darurat
   Dalam situasi darutat, SIAK-CSIRT berwenang memberikan rekomendasi teknis maupun non-teknis kepada pimpinan dan unit kerja terkait untuk pemulihan, mitigasi dan pencegahan insiden serupa di masa mendatang.
5. Memberikan rekomendasi tindak lanjut
   SIAK-CSIRT berwenang memberikan rekomendasi teknis maupun non-teknis kepada pimpinan dan unit kerja terkait untuk pemulihan, mitigasi, dan pencegahan insiden serupa di masa mendatang
6. Membuat dan mendistribusikan laporan insiden
   SIAK-CSIRT memiliki otoritas untuk menyusun laporan penanganan insiden dan mendistribusikannya kepada pimpinan atau instansi yang berwenang

7. Menjaga kerahasiaan informasi insiden
   Tim memiliki otoritas untuk mengelola informasi terkait insiden siber dengan menjaga kerahasiaan, integritas dan akurasi informasi sesuai dengan kebijakan organisasi

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

Nama-CSIRT melayani penanganan insiden siber dengan jenis berikut :

a. Ransomware

Dukungan Tim CSIRT:

- **Deteksi dan Konfirmasi Awal:** Mengidentifikasi sistem yang terinfeksi ransomware dan jenis variannya.
- **Isolasi Sistem:** Memutus koneksi jaringan pada perangkat yang terdampak untuk mencegah penyebaran.
- **Analisis Forensik:** Menelusuri sumber serangan dan metode infeksi.
- **Pemulihan Sistem:** Melakukan restorasi dari backup yang aman.
- **Koordinasi Eksternal:** Berkoordinasi dengan lembaga seperti BSSN dan vendor keamanan untuk update kunci dekripsi (jika tersedia).
- **Edukasi Pengguna:** Sosialisasi bahaya membuka lampiran mencurigakan atau tautan tidak dikenal.

b. Malware

Dukungan Tim CSIRT:

- **Pemindaian dan Analisis Malware:** Menggunakan tools antivirus dan antimalware untuk identifikasi file berbahaya.
- **Isolasi dan Pembersihan:** Mengisolasi sistem terinfeksi dan melakukan pembersihan malware.
- **Update Sistem:** Menyediakan patch keamanan untuk menutup celah yang dimanfaatkan malware.
- **Monitoring Lanjutan:** Memasang IDS/IPS untuk memantau potensi infeksi ulang.
- **Pelaporan dan Dokumentasi:** Menyusun laporan teknis terkait insiden dan langkah mitigasi.

c. Ddos

Dukungan Tim CSIRT:

- **Identifikasi Lalu Lintas Tidak Normal:** Menganalisis log dan trafik untuk mendeteksi volume serangan.
- **Mitigasi Teknis:** Bekerja sama dengan ISP untuk memfilter atau memblokir trafik jahat (blackhole routing, rate-limiting).
- **Pengaktifan Proteksi Cloud/Firewall:** Mengalihkan layanan melalui anti-DDoS protection (Cloudflare, Akamai, dsb).
- **Koordinasi Cepat:** Menyampaikan notifikasi kepada pemilik sistem dan instansi terkait.
- **Pemulihan dan Evaluasi:** Memulihkan layanan dan melakukan review pasca serangan.

d. Serangan Phising

Dukungan Tim CSIRT :

- **Analisis Email Phishing:** Menelusuri header, konten, dan tautan berbahaya dalam email.
- **Blokir Domain dan Akses:** Memblokir URL phishing di firewall, proxy, atau DNS.
- **Peringatan ke Pengguna:** Mengirimkan alert kepada seluruh pegawai agar tidak membuka email serupa.
- **Pelaporan ke Pihak Eksternal:** Melaporkan situs phishing ke penyedia domain atau CERT nasional.
- **Pelatihan Pengguna:** Edukasi rutin tentang cara mengenali dan melaporkan email phishing.

e. SQL Injection

Dukungan Tim CSIRT:

- **Deteksi Celah Aplikasi:** Menguji dan mengidentifikasi parameter atau formulir web yang rentan.
- **Koordinasi dengan Developer:** Memberikan rekomendasi teknis untuk sanitasi input dan parameterisasi query.
- **Pemantauan Log Database:** Memeriksa akses dan query mencurigakan.
- **Penutupan Sementara Layanan:** Jika dibutuhkan, menghentikan sementara layanan untuk mencegah eksploitasi lebih lanjut.
- **Uji Keamanan Ulang:** Melakukan retesting aplikasi setelah perbaikan dilakukan.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Kerjasama dan berbagi informasi antara SIAK-CSIRT dalam lingkup keamanan siber mencakup :

a. Pertukaran informasi teknis
   mengenai indikator kompromi (IoC), taktik dan teknik serangan serta metode mitigas
b. Pemberian bantuan teknis saat terjadi insiden
c. Koordinasi respons insiden antar organisasi atau lintas sektor
d. Pelatihan bersama atau simuliasi penanganan insiden (*cyber drill*)
e. Penyusunan kebijakan bersama dalam menangani ancaman tertentu

SIAK-CSIRT sangart menjunjung tinggi prinsip kerahasiaan informasi. Data atau informasi yang dikumpulkan dan dibagikan akan diperlakukan sesuai dengan klasifikasi dan sensitivitasnya. Beberapa prinsip yang diberikan antara lain :

a. Informasi sensitif tidak akan diungkapkan kepada pihak luar tanpa izin tertulis dari pihak yang memilikinya
b. Anonimisasi data dapat dilakukan sebelum berbagi ke pihak ketiga, agar tidak mengungkapkan identitas organisasi atau individu terkait

c. Perjanjian Non-Disclosure Agreement (NDA) atau nota kesepakatan (MoU) akan digunakan jika diperlukan untuk memastikan kepatuhan terkait kerahasiaan data
d. Hanya informasi yang relevan dan diperlukan untuk kepentingan respons dan mitigasi yang akan dibagikan

4.3. Komunikasi dan Autentikasi

Komunikasi

- **Saluran Komunikasi Resmi**
  Email khusus CSIRT, portal incident management, aplikasi ticketing (contoh: OTRS, OSTicket), dan dashboard monitoring (misalnya: SIEM, Wazuh, Zabbix).
- **Komunikasi Internal**
  Digunakan untuk koordinasi penanganan insiden, berbagi update status, dan dokumentasi teknis. Bisa menggunakan chat aman (Signal, Mattermost) atau intranet.
- **Komunikasi Eksternal**
  Untuk berhubungan dengan BSSN, CSIRT lain, vendor keamanan, atau publik (press release). Umumnya menggunakan kanal yang terproteksi.
- **Prinsip Keamanan**
  Mengutamakan kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) dalam setiap pertukaran informasi.

Autentikasi memastikan bahwa orang yang berkomunikasi benar-benar pihak yang berwenang. Beberapa mekanismenya:

- **Autentikasi Multi-Faktor (MFA):**
  Kombinasi password + OTP (One Time Password) atau token fisik/digital.
  Sertifikat Digital & PKI (Public Key Infrastructure):
  Digunakan untuk email signing/encryption (PGP, S/MIME) agar pesan tidak bisa dipalsukan.
- VPN / Tunneling
  Akses ke sistem CSIRT internal (misalnya dashboard insiden atau repository forensik) hanya bisa dilakukan melalui koneksi terenkripsi.
- Role-Based Access Control (RBAC):
  Setiap anggota CSIRT hanya bisa mengakses data sesuai dengan perannya (misalnya, analis insiden, koordinator, atau forensik).
- Autentikasi dengan Sistem Terpusat:
  Menggunakan LDAP, Active Directory, atau Identity Provider untuk single sign-on (SSO).

5. Layanan

5.1. Layanan Utama

Layanan utama dari SIAK-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini berupa penyampaian informasi dini kepada perangkat daerah atau instansi terkait mengenai adanya potensi ancaman siber, kerentanan, maupun aktivitas mencurigakan yang dapat berdampak pada sistem elektronik Pemerintah Kabupaten Siak. Peringatan ini dapat berbentuk *early warning* atau *security advisory* sehingga organisasi dapat melakukan langkah pencegahan sebelum insiden terjadi.

5.1.2. Penanganan Insiden Siber

Merupakan layanan inti CSIRT dalam merespon insiden keamanan siber yang terjadi pada sistem elektronik lingkup Pemkab Siak. Proses ini meliputi identifikasi, analisis, mitigasi, pemulihan, serta dokumentasi insiden. Tujuannya adalah meminimalisasi dampak insiden, memulihkan layanan, serta memberikan rekomendasi pencegahan agar kejadian serupa tidak terulang.

5.2. Layanan Tambahan

Layanan tambahan dari SIAK-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini mencakup kegiatan identifikasi dan perbaikan kerentanan pada aplikasi, jaringan, atau infrastruktur TIK yang digunakan oleh perangkat daerah. CSIRT dapat melakukan asesmen keamanan (misalnya vulnerability assessment) serta memberikan rekomendasi perbaikan kepada pengelola sistem elektronik.

5.2.2. Penanganan Artefak Digital

Layanan ini berfokus pada pengumpulan, analisis, dan pelestarian bukti digital terkait insiden siber. Artefak digital seperti log, file mencurigakan, atau malware dianalisis untuk mengetahui pola serangan, teknik yang digunakan penyerang, serta potensi dampaknya.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

CSIRT melakukan monitoring proaktif terhadap tren ancaman siber, baik secara global maupun nasional, kemudian menyampaikan hasil pengamatan tersebut kepada perangkat daerah. Informasi ini berguna untuk meningkatkan kesiapan organisasi dalam menghadapi serangan.

5.2.4. Pendeteksian Serangan

Layanan ini dilakukan dengan memanfaatkan sistem monitoring, IDS/IPS, SIEM, maupun log sistem untuk mendeteksi aktivitas serangan secara dini. Tujuannya agar insiden dapat ditangani lebih cepat sebelum menimbulkan kerusakan yang lebih besar.

5.2.5. Analisis Risiko Keamanan Siber

CSIRT membantu perangkat daerah dalam melakukan identifikasi, evaluasi, dan penilaian risiko terhadap sistem elektronik. Hasil analisis digunakan sebagai dasar dalam menentukan prioritas pengamanan, alokasi sumber daya, serta strategi mitigasi risiko.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

CSIRT menyediakan layanan konsultasi untuk perangkat daerah yang ingin meningkatkan kesiapan menghadapi insiden. Layanan ini bisa berupa asistensi penyusunan prosedur respons insiden, penyusunan playbook, maupun pendampingan dalam simulasi insiden (cyber drill).

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini berupa kegiatan edukasi, sosialisasi, dan pelatihan bagi aparatur pemerintah daerah mengenai pentingnya keamanan siber. Tujuannya adalah menumbuhkan budaya sadar keamanan (security awareness) sehingga risiko insiden akibat kelalaian manusia dapat ditekan.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@mail.siakkab.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*

SIAK-CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada Perangkat Daerah di lingkungan Pemerintah Kabupaten Siak. Penanganan insiden siber dilakukan sesuai dengan kapasitas serta ketersediaan tools yang dimiliki.

Setiap tindak pencegahan dilakukan melalui penyusunan informasi, pemberitahuan, dan peringatan. Dengan demikian, SIAK-CSIRT tidak bertanggung jawab atas kesalahan, kelalaian, maupun kerusakan yang timbul akibat penggunaan informasi yang terdapat di dalamnya.

Selain itu, SIAK-CSIRT tidak memiliki kewenangan dalam penyelesaian persoalan hukum yang mungkin muncul terkait dengan insiden keamanan siber.