

RFC 2350 OKUSKab-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 2.0 yang diterbitkan pada tanggal 01 Agustus 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.okuselatankab.go.id/index.php/rfc-2350/>

1.4. Keaslian Dokumen

Dokumen telah ditandatangani dengan sertifikat elektronik milik Dinas Komunikasi dan Informatika Kabupaten Ogan Komering Ulu Selatan

1.5. Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 OKUSKab-CSIRT

Versi : 2.0

Tanggal Publikasi : 19 Agustus 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 Ogan Komering Ulu Selatan. Disingkat : OKUSKab-CSIRT

2.2. Alamat

Dinas Komunikasi dan Informatika kabupaten Ogan Komering Ulu Selatan Jl. Serasan Seandanan No. 17 Muaradua Ogan Komering Ulu Selatan Sumatera Selatan, 32211.

2.3. Zona Waktu

Muaradua (GMT+07:00)

2.4. Nomor Telepon

1. 0821 1286 4893
2. 0821 8247 7564

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak ada

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

csirt.okuselatankab.go.id

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

Bits : 4096-bit

ID : csirt okuskab <csirt@okuselatankab.go.id>

Key Fingerprint : 4379 04E4 470A DDFC FBE9 35BB 49A9 3D1C B02A 91A1

https://drive.google.com/file/d/1IC2FdgwX_hpnwOwglcVNz6O0pdYynK0g/view?usp=sharing

File PGP key ini tersedia pada : <https://csirt.okuselatankab.go.id/index.php/rfc-2350/>

2.9. Anggota Tim

Ketua OKUSKab-CSIRT adalah Kepala Dinas Komunikasi dan Informatika yang termasuk anggota tim adalah seluruh staf Dinas Komunikasi dan Informatika dan Organisasi Perangkat Daerah Kabupaten Ogan Komering Ulu Selatan, adalah sebagai agen penanganan insiden siber pada Pemerintah Kabupaten Ogan Komering Ulu Selatan.

2.10. Informasi/Data lain

Tidak ada

2.11. Catatan-catatan pada Kontak OKUSKab-CSIRT

Metode yang disarankan untuk menghubungi OKUSKab-CSIRT adalah melalui *e-mail* pada alamat email : csirt@okuselatankab.go.id. atau melalui nomor telepon 982182477564 pada hari kerja jam 07.30 - 15.30 (Senin-Kamis) dan 07.30 - 14.30 (Jumat).

3. Mengenai OKUSKab-CSIRT

3.1. Visi

Visi dari (OKUSKab-CSIRT), yaitu :

“Menjadi Tim Tanggap Insiden Siber yang profesional, responsif, andal, dan terpercaya dalam mewujudkan penyelenggaraan keamanan siber yang tangguh guna mendukung Sistem Pemerintahan Berbasis Elektronik (SPBE) di lingkungan Pemerintah Kabupaten Ogan Komering Ulu Selatan.”

3.2. Misi

Misi dari (OKUSKab-CSIRT), yaitu :

- a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber pada pemerintahan Kabupaten Ogan Komering Ulu Selatan;
- b. Membangun Kapasitas Sumber daya Keamanan siber pada Pemerintah Kabupaten Ogan Komering Ulu Selatan;
- c. melakukan koordinasi dan kerja sama dalam rangka mencegah dan/atau mengurangi dampak dari Insiden Siber pada konstituen.

3.3. Konstituen

Konstituen OKUSKab-CSIRT meliputi Organisasi Pemerintah Daerah (OPD) dilingkungan Pemerintah Kabupaten Ogan Komering Ulu Selatan yang menggunakan layanan Data Senter Pemerintah Kabupaten Ogan Komering Ulu Selatan.

3.4. Sponsorship dan/atau Afiliasi

OKUSKab-CSIRT merupakan bagian dari Pemerintah Kabupaten Ogan Komering Ulu Selatan sehingga seluruh pembiayaan bersumber dari APBD Dinas Komunikasi dan Informatika Kabupaten Ogan Komering Ulu Selatan

3.5. Otoritas

OKUSKab-CSIRT memiliki kewenangan untuk melaksanakan penanggulangan insiden keamanan siber, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Pemerintah Kabupaten Ogan Komering Ulu Selatan. Dalam menjalankan tugasnya, OKUSKab-CSIRT berwenang melakukan koordinasi dengan konstituen dan instansi terkait dalam rangka penanganan insiden keamanan siber. Pelaksanaan penanggulangan dan pemulihan insiden dilakukan berdasarkan permintaan dari konstituen OKUSKab-CSIRT sesuai dengan mekanisme dan ketentuan yang berlaku.

4. Kebijakan – Kebijakan

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

OKUSKab-CSIRT memberikan layanan penanganan terhadap insiden keamanan siber yang terjadi pada konstituen di lingkungan Pemerintah Kabupaten Ogan Komering Ulu Selatan, meliputi:

- a. *Web Defacement*;
- b. *Distributed Denial of Service (DDoS)*;
- c. *Malware*; dan
- d. *Ransomware*

Tingkat atau level dukungan yang diberikan oleh OKUSKab-CSIRT kepada konstituen disesuaikan dengan jenis, tingkat keparahan (*severity*), ruang lingkup, serta dampak insiden yang terjadi, dengan mempertimbangkan ketersediaan sumber daya dan layanan yang terdampak. Dalam pelaksanaan penanganan insiden, OKUSKab-CSIRT dapat memberikan dukungan berupa :

1. Identifikasi dan verifikasi insiden;
2. Analisis dan asesmen dampak insiden;
3. Rekomendasi langkah mitigasi dan penanganan insiden;
4. Koordinasi penanganan insiden dengan konstituen dan pihak terkait;
5. Pendampingan proses pemulihan (*recovery*) layanan; dan
6. Penyusunan laporan hasil penanganan insiden serta rekomendasi pencegahan agar insiden serupa tidak terulang.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

OKUSKab-CSIRT melaksanakan kerja sama, koordinasi, dan pertukaran Informasi dengan **CSIRT Provinsi Sumatera Selatan, Badan Siber dan Sandi Negara (BSSN)** selaku **Government CSIRT (Gov-CSIRT)**, **Tim Tanggap Insiden Siber (TTIS)**, serta organisasi atau pihak lain yang bergerak di bidang keamanan siber sesuai dengan kewenangan dan kebutuhan penanganan insiden keamanan siber. Dalam pelaksanaan kerja sama tersebut, setiap informasi dan/atau data yang diterima, dikelola, maupun dipertukarkan oleh OKUSKab-CSIRT wajib dijaga kerahasiaannya serta hanya digunakan untuk kepentingan penanganan insiden keamanan siber sesuai dengan ketentuan peraturan perundang-undangan dan kebijakan keamanan informasi yang berlaku. Apabila terdapat pengungkapan informasi kepada pihak lain, pengungkapan tersebut hanya dapat dilakukan

berdasarkan persetujuan pihak yang berwenang dan sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

4.3. Komunikasi dan Autentikasi

Dalam pelaksanaan layanan, OKUSKab-CSIRT menggunakan media komunikasi yang disesuaikan dengan tingkat klasifikasi informasi yang disampaikan. Untuk komunikasi yang bersifat umum, OKUSKab-CSIRT menggunakan surat elektronik (*e-mail*) konvensional, telepon, dan media komunikasi resmi lainnya. Sementara itu, untuk komunikasi yang memuat informasi sensitif, terbatas, atau rahasia terkait penanganan insiden keamanan siber, OKUSKab-CSIRT menggunakan mekanisme pengamanan komunikasi melalui enkripsi **Pretty Good Privacy (PGP)** pada surat elektronik (*e-mail*) atau metode pengamanan lainnya sesuai dengan kebijakan keamanan informasi dan ketentuan yang berlaku.

5. Layanan dan Fungsi

5.1. Layanan

Layanan dari OKUSKab-CSIRT yaitu :

5.1.1. Penanggulangan Dan Pemulihan Insiden Siber

TTIS memiliki peran penting dalam melakukan penanggulangan dan pemulihan dengan melakukan kegiatan mendeteksi, merespons, dan mengatasi insiden keamanan siber. Berikut adalah beberapa layanan dalam konteks penanggulangan dan pemulihan 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. Penyampaian informasi insiden siber kepada pihak terkait

Pemberian informasi insiden siber bertujuan untuk memberikan informasi dan peringatan yang relevan tentang potensi ancaman atau kerentanan keamanan siber kepada pemilik sistem elektronik. Pemberian informasi penting dalam membantu organisasi untuk

membantu pihak terkait dalam merespons ancaman dengan cepat dan efektif.

5.1.3. Diseminasi Informasi Untuk Mencegah dan/atau Mengurangi Dampak dari Insiden Siber

Diseminasi informasi penting dalam membantu organisasi untuk menjaga keamanan informasi dalam upaya mencegah dan/atau mengurangi dampak dari insiden siber. Dengan informasi yang tepat, penyelenggara sistem elektronik dapat menyusun kebijakan dan melakukan tindakan yang sesuai guna mengurangi risiko dan merespons insiden keamanan siber dengan lebih baik.

5.2. Fungsi

5.2.1. Fungsi Utama atas layanan OKUSKab-CSIRT

5.2.1.1. Pemberian peringatan terkait Keamanan Siber;

Layanan ini dilaksanakan oleh OKUSKab-CSIRT berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan Informasi statistik terkait layanan ini diberikan oleh OKUSKab-CSIRT

5.2.1.2. Perumusan panduan teknis penanganan Insiden Siber;

OKUSKab-CSIRT menyusun dan mengembangkan panduan teknis penanganan Insiden Siber sebagai acuan bagi konstituen dalam melakukan pencegahan, penanganan, pemulihan, dan peningkatan keamanan sistem elektronik

5.2.1.3. Pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak; OKUSKab-CSIRT melakukan pencatatan terhadap setiap laporan atau aduan Insiden Siber yang diterima, serta memberikan rekomendasi langkah-langkah penanganan awal kepada pihak yang terdampak guna meminimalkan dampak yang ditimbulkan.

5.2.1.4. Pemilahan (triage) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani; OKUSKab-CSIRT melakukan proses pemilahan (triage) terhadap setiap Insiden Siber berdasarkan tingkat urgensi, dampak, dan kriteria yang telah ditetapkan untuk menentukan prioritas penanganan.

5.2.1.5 Penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan; dan OKUSKab-CSIRT menyelenggarakan koordinasi penanganan Insiden Siber dengan pihak-pihak terkait, baik internal maupun eksternal, guna memastikan penanganan insiden berjalan secara efektif dan terintegrasi.

- 5.2.1.6.** Diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.
OKUSKab-CSIRT melaksanakan diseminasi informasi, edukasi, dan peningkatan Keamanan Siber kepada konstituen sebagai upaya pencegahan dan pengurangan dampak yang ditimbulkan oleh Insiden Siber.

5.2.2. Fungsi Lain atas layanan OKUSKab-CSIRT

5.2.2.1 Penanganan Kerawanan Sistem Elektronik

Layanan **Penanganan Kerawanan Sistem Elektronik** diberikan oleh **OKUSKab-CSIRT** dalam bentuk koordinasi, pendampingan teknis, dan pemberian rekomendasi penguatan keamanan (*system hardening*) terhadap sistem elektronik milik konstituen guna mengurangi risiko terjadinya insiden keamanan siber.

Layanan ini diberikan dengan ketentuan sebagai berikut:

- a. Pelapor kerawanan merupakan pemilik atau penanggung jawab sistem elektronik yang menjadi objek pelaporan. Apabila pelapor bukan merupakan pemilik atau penanggung jawab sistem elektronik dimaksud, maka laporan kerawanan tidak dapat ditindaklanjuti oleh OKUSKab-CSIRT;
- b. Penanganan kerawanan sistem elektronik dapat dilakukan berdasarkan laporan dari konstituen atau sebagai tindak lanjut atas hasil kegiatan **Vulnerability Assessment** yang dilaksanakan oleh OKUSKab-CSIRT maupun pihak yang berwenang;
- c. OKUSKab-CSIRT memberikan rekomendasi teknis berupa langkah-langkah mitigasi dan penguatan keamanan (*hardening*) sesuai dengan tingkat kerawanan yang ditemukan; dan
- d. Pelaksanaan perbaikan terhadap kerawanan sistem elektronik menjadi tanggung jawab pemilik atau pengelola sistem elektronik, dengan pendampingan dan koordinasi dari OKUSKab-CSIRT apabila diperlukan.

5.2.2.2. Penanganan Artefak Digital

Layanan ini diberikan oleh OKUSKab-CSIRT berupa penanganan artefak dalam rangka pemulihan sistem elektronik berdampak ataupun dukungan Investigasi

OKUSKab-CSIRT Memberikan Informasi statistic terkait layanan ini.

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. OKUSKab-CSIRT memberikan informasi kepa 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. OKUSKab-CSIRT memberikan informasi terkait layanan ini.

5.2.2.5. Analisis Risiko Keamanan Siber

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

5.2.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini diberikan OKUSKab-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

OKUSKab-CSIRT melaksanakan, mendokumentasikan, dan mempublikasikan kegiatan Dinas Komunikasi dan Informatika Kabupaten/Kota xxx dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber.

6. Pelaporan Insiden

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

- a. Foto/*scan* kartu identitas
- b. Bukti insiden berupa foto atau *screenshot* atau *log file* yang ditemukan
- c. Atau sesuai dengan ketentuan lain yang berlaku

7. Disclaimer

- a. OKUSKab-CSIRT hanya merespon dan menangani insiden keamanan siber yang terjadi pada Perangkat Daerah di Lingkungan Pemerintah Kabupaten Ogan Komering Ulu Selatan.
- b. Terkait penanganan insiden siber tergantung dari ketersediaan *tools* yang dimiliki;

- c. Setiap tindak pencegahan akan diambil dalam penyusunan informasi, pemberitahuan dan peringatan, maka OKUSKab-CSIRT tidak bertanggung jawab atas kesalahan dan kelalaian atau kerusakan yang diakibatkan dari penggunaan informasi yang terkandung dalamnya. OKUSKab-CSIRT juga tidak memiliki wewenang dalam persoalan hukum.