

RFC 2350 EDU-CSIRT KEMENDIKBUDRISTEK

1. Informasi mengenai dokumen ini berisi deskripsi Edu-CSIRT Kemendikbudristek berdasarkan RFC 2350, yaitu informasi dasar mengenai Edu-CSIRT Kemendikbudristek, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi Edu-CSIRT Kemendikbudristek.
 - 1.1. Tanggal update terakhir dokumen merupakan dokumen versi 1.2 yang diterbitkan pada tanggal 2 Maret 2023
 - 1.2. Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.
 - 1.3. Lokasi dimana dokumen ini bisa didapat versi terbaru dari dokumen ini tersedia pada web <https://educsirt.kemdikbud.go.id>
 - 1.4. Keaslian kedua dokumen (versi bahasa inggris dan bahasa Indonesia) adalah dokumen yang telah ditanda tangani Kepala Pusat Data dan Teknologi Informasi (PUSDATIN) Kemendikbudristek
 - 1.5. Identifikasi dokumen kedua dokumen (versi bahasa inggris dan bahasa Indonesia) memiliki atribut yang sama, yaitu:
 - 1.5.1. Judul : RFC 2350 EDU-CSIRT KEMENDIKBUDRISTEK
 - 1.5.2. Versi : 1.2
 - 1.5.2. Tanggal Publikasi : 2 Maret 2023
 - 1.5.3. Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.
2. Informasi Data/Kontak
 - 2.1. Nama Tim Education-Computer Security Incident Response Team Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi disingkat dengan Edu-CSIRT Kemendikbudristek.
 - 2.2. Alamat Pusat Data dan Teknologi Informasi Kemendikbudristek Jl. RE Martadinata Cipayung, Ciputat, Tangerang Selatan, Banten, Indonesia.
 - 2.3. Zona Waktu Jakarta (GMT+07:00)
 - 2.4. Nomor Telepon (021) 7418808,
 - 2.5. Nomor Fax (021)7401727
 - 2.6. Nomor Helpdesk Edu-CSIRT Kemendikbudristek 08111977478
 - 2.6. Alamat Surat Elektronik (E-mail) [educsirt\[at\]kemdikbud.go.id](mailto:educsirt[at]kemdikbud.go.id)
 - 2.7. Anggota Tim

Ketua Edu-CSIRT Kemendikbudristek adalah Kepala Pusat Data dan Teknologi Informasi (Pusdatin) Kemendikbudristek dengan anggota tim adalah seluruh staf Bidang Substansi Aplikasi dan Keamanan Informasi, Tata Kelola TIK, Data dan Statistik Pendidikan, Data

Kebudayaan dan Kebahasaan Pusdatin dan perwakilan dari satuan kerja di unit Kemendikbudristek.

2.8. Informasi/data lain

Tidak ada.

2.9. Catatan-catatan pada Kontak Edu-CSIRT Kemendikbudristek

Metode yang disarankan untuk menghubungi Edu-CSIRT Kemendikbudristek adalah melalui e-mail pada alamat [educsirt\[at\]kemdikbud.go.id](mailto:educsirt[at]kemdikbud.go.id) atau melalui nomor telepon (08111977478) ke Edu- CSIRT Kemendikbudristek yang siaga selama 24/7.

3. Mengenai Edu-CSIRT

3.1. Visi Edu-CSIRT Kemendikbudristek adalah terwujudnya ketahanan siber pada sektor pendidikan yang handal dan profesional.

3.2. Misi dari Edu-CSIRT Kemendikbudristek, yaitu :

3.2.1. Mengkoordinasikan dan mengolaborasikan layanan keamanan siber pada sektor pemerintah khususnya sektor pendidikan baik internal dan eksternal

3.2.2. Mengidentifikasi kerentanan keamanan secara menyeluruh

3.2.3. Meningkatkan respon aspek keamanan kepada seluruh Satuan Unit Kerja Kemendikbudristek

3.2.4. Meningkatkan mutu layanan TIK Pendidikan, Kebudayaan, Riset dan Teknologi dari acaman siber.

3.3. Konstituen

Konstituen Edu-CSIRT Kemendikbudristek adalah seluruh satuan unit kerja Kemendikbudristek

3.4. Sponsorship dan/atau Afiliasi

Sponsorship dan/atau Afiliasi Edu-CSIRT Kemendikbudristek merupakan bagian dari Pusdatin Kemendikbudristek sehingga seluruh pembiayaan bersumber dari APBN.

4. Kebijakan–Kebijakan

4.1. Jenis-jenis insiden dan tingkat/level Dukungan Edu-CSIRT Kemendikbudristek memiliki otoritas untuk menangani insiden yaitu:

- a. Web Defacement;
- b. DDoS;
- c. Malware;
- d. Phising;
- e. Pembajakan akun

f. Akses Ilegal

g. Spam

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Edu-CSIRT Kemendikbudristek akan melakukan kerjasama dan berbagi informasi dengan CSIRT dari Kementerian dan atau Lembaga lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh Edu-CSIRT Kemendikbudristek akan dirahasiakan.

4.3. Komunikasi dan Autentikasi untuk komunikasi biasa Edu-CSIRT Kemendikbudristek dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon.

4.4. Komunikasi terkait laporan insiden dan pertukaran informasi ancaman insiden lainnya dapat menggunakan saluran komunikasi yang disediakan (e-mail, whatsapp, call center) yang telah terenkripsi atau dilengkapi dengan kata sandi.

5. Layanan

5.1. Layanan Reaktif

Layanan reaktif dari Edu-CSIRT Kemendikbudristek merupakan layanan utama dan bersifat prioritas, yaitu:

5.1.1. Layanan pemberian peringatan terkait dengan laporan insiden siber

Layanan ini dilaksanakan oleh Edu-CSIRT Kemendikbudristek berupa pemberian peringatan adanya insiden siber pada sistem elektronik dan informasi statistik yang dikelola oleh masing-masing satuan kerja Kemendikbudristek

5.1.2. Layanan penanggulangan dan pemulihan Insiden

Layanan ini diberikan oleh Edu-CSIRT Kemendikbudristek berupa koordinasi, analisis, rekomendasi teknis, dan bantuan kunjungan ke lokasi dalam rangka penanggulangan dan pemulihan insiden siber. Edu-CSIRT Kemendikbudristek memberikan informasi statistik terkait layanan ini.

5.1.3. Layanan penanganan kerawanan

Layanan ini diberikan oleh Edu-CSIRT Kemendikbudristek berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*), Edu-CSIRT Kemendikbudristek memberikan informasi statistik terkait layanan ini. 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 oleh Edu-CSIRT Kemendikbudristek berupa penanganan artifak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi. Edu-CSIRT Kemedikbudristek memberikan informasi statistik terkait layanan ini

5.2. Layanan Proaktif

Edu-CSIRT Kemendikbudristek secara aktif membangun kapasitas sumber daya keamanan siber melalui kegiatan:

5.2.1. Pemberitahuan hasil pengamatan terkait dengan ancaman baru Layanan ini diberikan oleh Edu-CSIRT Kemendikbudristek berupa hasil dari sistem deteksi dini sistem monitoring keamanan. Edu-CSIRT Kemendikbudristek memberikan informasi statistik terkait layanan ini.

5.2.2. Layanan security assessment

Layanan ini diberikan oleh Edu-CSIRT Kemendikbudristek berupa identikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan. Edu-CSIRT Kemendikbudristek memberikan informasi statistik terkait layanan ini.

5.2.3. Layanan security audit

Layanan ini diberikan oleh Edu-CSIRT Kemendikbudristek berupa penilaian keamanan informasi. Edu-CSIRT Kemendikbudristek memberikan informasi statistik terkait layanan ini.

5.2.4. Layanan Manajemen

Kualitas Keamanan Edu-CSIRT Kemendikbudristek meningkatkan kualitas keamanan melalui kegiatan:

- a. Konsultasi terkait kesiapan penanggulangan dan pemulihan Insiden
- b. Layanan ini diberikan oleh Edu-CSIRT Kemendikbudristek berupa pemberian rekomendasi teknis berdasarkan hasil analisis terkait penanggulangan dan pemulihan insiden
- c. Pembangunan kesadaran dan kepedulian terhadap keamanan siber
- d. Dalam layanan ini Edu-CSIRT Kemendikbudristek mendokumentasikan dan mempublikasikan berbagai kegiatan yang dilakukan dalam rangka pembangunan kesadaran dan kepedulian terhadap keamanan siber
- e. Pembinaan terkait kesiapan penanggulangan dan pemulihan insiden

- f. Edu-CSIRT Kemendikbudristek menyiapkan program pembinaan dalam rangka pendukung penanggulangan dan pemulihan insiden

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke [educsirt\[at\]kemdikbud.go.id](mailto:educsirt[at]kemdikbud.go.id) dengan melampirkan sekurang-kurangnya:

- a. Foto/*scan* kartu identitas
- b. Bukti insiden berupa foto atau *screenshot* atau *log file* yang ditemukan

7. *Disclaimer* terkait penanganan jenis *malware* tergantung dari ketersediaan *tools* yang dimiliki.