RFC 2350 DPD RI-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 12 Maret 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 :
CSIRT 2025 versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 DPDRI-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 12 Maret 2025;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan

2. Informasi Data/Kontak

2.1. Nama Tim

Tim Tanggap Insiden Keamanan Siber (Computer Security Incident Response Team) Dewan Perwakilan Daerah Republik Indonesia yang selanjutnya disebut DPDRI-CSIRT.

2.2. Alamat

DPD RI-CSIRT
Kompleks Parlemen MPR/DPR/DPD RI
Jl. Jend. Gatot Soebroto No.6,
Senayan - 12550, Jakarta

2.3. Zona Waktu

Ibukota DKI Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 57897371

2.5. Nomor Fax

(021) 57897371

2.6. Telekomunikasi Lain

Tidak ada

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

csirt@dpd.go.id

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

Bits : 4.096
ID : 7967AEB3EB37628D
Key Fingerprint : 53EE8048EA873D1F23AA74287967AEB3EB37628D

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

xjMEZvUM2hYJKwYBBAHaRw8BAQdAgUXhqST7z9i0bwDUTJJPpEwM9YlFjwrotEZ+
ppTIMRrNJUNTSVJUIFNFVEpFTiBEUEQgUkkgPGNzaXJ0QGRwZC5nby5pZD7CmQQT
FgoAQRYhBFPugEjqhz0fI6p0KHlnrrPrN2KNBQJm9QzaAhsDBQkFo3f2BQsJCAcC
AiICBhUKCQgLAgQWAgMBAh4HAheAAAoJEHlnrrPrN2KNgXoBAPqA9gL4u40XWSNK
aMHglgo7/9/omPJ9bpOsogEPAwwcAP9c3HtAJrprjpn8bKZROah6Xm53P0L6d6RM
rQ/pMIipBc44BGb1DNoSCisGAQQBl1UBBQEBB0D5U1PMNV88yERNyBR4LvtoKkKB
x3VXZ5ZpNEFLS+/ISwMBCAfCfgQYFgoAJhYhBFPugEjqhz0fI6p0KHlnrrPrN2KN
BQJm9QzaAhsMBQkFo3f2AAoJEHlnrrPrN2KNTYsBAKbDY5MuQyoQrSL7KA8zV+oX
8FO4TFmxfWRSAAZ0Z37kAQCf8Y/HZHshKNYIOtMGRGZTzYfOLwbbD6K9vZNoTwb5
Cg==
=ooFk
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://keys.openpgp.org/vks/v1/by-fingerprint/7124CDD5E92F672596741B792E2966439E4571F7

2.9. Anggota Tim

Pengarah DPD RI-CSIRT adalah Sekretaris Jenderal DPD RI, Ketua DPD RI-CSIRT adalah Deputi Bidang Administrasi, Sekretaris DPD RI-CSIRT adalah Kepala Biro Sistem Informasi dan Dokumentasi, dan anggotanya merupakan Pegawai yang menangani insiden siber / teknologi informasi di Bagian Pengelolaan Sistem Informasi, Biro Sistem Informasi dan Dokumentasi, Sekretariat Jenderal DPD RI.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak Nama-CSIRT

Metode yang disarankan untuk menghubungi DPD RI-CSIRT adalah melalui *e-mail* pada alamat csirt@dpd.go.id atau melalui nomor telepon (021) 57897371 ke Bagian Pengelolaan Sistem Informasi, Biro Sistem Informasi dan Dokumentasi.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi DPDRI-CSIRT adalah terwujudnya ketahanan siber di lingkungan Sekretariat Jenderal DPD RI yang andal dan profesional.

3.2. Misi

Misi dari DPDRI-CSIRT, yaitu :

Tujuan dari DPDRI-CSIRT**, yaitu :**

a. Membangun, mengoordinasikan, mengolaborasikan dan melaksanakan layanan DPDRI_CSIRT, Manajemen Insiden, penanggulangan dan pemulihan terhadap insiden keamanan siber di Lingkungan Sekretariat Jenderal Dewan Perwakilan Daerah Republik Indonesia;
b. Membangun dan melakukan kerja sama dalam rangka penanggulangan dan pemulihan insiden keamanan siber di Lingkungan Sekretariat Jenderal Dewan Perwakilan Daerah Republik Indonesia;
c. Mengembangkan dan mengoptimalkan kapasitas sumber daya penanggulangan dan pemulihan insiden keamanan siber di Lingkungan Sekretariat Jenderal Dewan Perwakilan Daerah Republik Indonesia;
d. Mendorong pelatihan dan keamanan siber di Lingkungan Sekretariat Jenderal Dewan Perwakilan Daerah Republik Indonesia.

3.3. Konstituen

Konstituen DPDRI-CSIRT meliputi :

a. Pimpinan dan Anggota Dewan Perwakilan Daerah Republik Indonesia;
b. Pegawai Sekretariat Jenderal Dewan Perwakilan Daerah Republik Indonesia;
c. Pegawai Kantor Perwakilan Dewan Perwakilan Daerah Republik Indonesia di Ibukota Provinsi.

3.4. Sponsorship dan/atau Afiliasi

DPDRI-CSIRT merupakan bagian dari Sekretariat Jenderal Dewan Perwakilan Daerah Republik Indonesia sehingga seluruh pembiayaan bersumber dari APBN.

3.5. Otoritas

DPDRI-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di Dewan Perwakilan Daerah Republik Indonesia.

DPDRI-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya dan dapat berkoordinasi serta melakukan eskalasi kepada pihak Badan Siber dan Sandi Negara (BSSN) / Pihak lainnya untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

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

DPDRI-CSIRT memiliki otoritas untuk menangani insiden yaitu :

a. Web Defacement;
b. Serangan DoS (Denial-of-service attack);
c. Malware;
d. Phising.

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

DPDRI-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh DPDRI-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

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

5. Layanan

5.1. Layanan Utama

Layanan utama dari DPDRI-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

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

5.1.2. Penanganan Insiden Siber

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

5.2. Layanan Tambahan

Layanan tambahan dari DPDRI-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan 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.

5.2.2. Penanganan Artefak Digital

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

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan berupa hasil dari sistem deteksi dini Honeynet BSSN. DPDRI-CSIRT memberikan informasi statistik terkait layanan ini.

5.2.4. Pendeteksian Serangan (*Security Assesment*)

Layanan ini berupa identikasi atas kerentanan yang ditemukan. DPDRI-CSIRT memberikan informasi statistik terkait layanan ini.

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini berupa penilaian/analisis risiko keamanan informasi. DPDRI-CSIRT Indonesia memberikan informasi dokumen/statistik terkait layanan ini.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini diberikan DPDRI-CSIRT berupa pemberian rekomendasi teknis berdasarkan hasil analisis terkait penanggulangan dan pemulihan insiden.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Dalam layanan ini DPDRI-CSIRT mendokumentasikan dan mempublikasikan berbagai kegiatan yang dilakukan dalam rangka pembangunan kesadaran dan kepedulian terhadapkeamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@dpd.go.id atau dengan mengisi *helpdesk* pada website https://csirt.dpd.go.id/ dengan melampirkan sekurang-kurangnya Bukti insiden berupa :

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*

Sebutkan jika ada.