RFC 2350 *DAHANA-CSIRT*

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 3.0 yang diterbitkan pada tanggal 04 Februari 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://dahana.id (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 *DAHANA-CSIRT*;
Versi : 2.0;
Tanggal Publikasi : *23 Februari 2026*;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Kepanjangan dari DAHANA-CSIRT

PT. Dahana – Computer Security Incident Response Team
Disingkat : *DAHANA-CSIRT*.

2.2. Alamat

Jl. Raya Subang Cikamurang KM 12 Cibogo, Subang, Jawa Barat 41285

2.3. Zona Waktu

Subang, Jawa Barat, Indonesia (GMT +07:00)

2.4. Nomor Telepon

+622607423333

2.5. Nomor Fax

Tidak ada

2.6. Telekomunikasi Lain

Tidak ada

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

csirt@dahana.id

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

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

xsFNBGmb+4YBEADY7l6O5XmdIhv2n22diNNs2b0lxfBFDk0rnfw6+ll3a9zVIfk5
HVDeG0V8KxPcpMGXN/XCaTDiWmhckAqhXSrVyG6lJI+x9VM3/MS7+SIOy8TcMcc3
Nl7kMp6YpVvW7Pqcq9QrrczHGGKAX9wO/e1I1O70nSnoJKA2+MOJH4sU7+urzeFq
6wT4U/EO02/k29nKg9oNoedeZNpTwRX3eoHFuSECifkoa3pRkWJXRMv5Bn5+LVU4
O7t6fiFr1TpXJG5FkJC8fGZAu6iOYKBtBhFQXSPD8OWvkbtZAKE+l1PTM1zZoX6w
uObjzukhxhfzrt7rz7gmqrTt8LD9l4cnL/SnEE1nYZ2/g1Dyta8sHjU6x0jUoqJh
7QlH9fsv2nqD34oVN0B+h8IRfy3/WzOpqBflHFB/Rq4RMA7w2RgGtRO9/NpLzX7c
znuEBxq0iYdFR0w4QLPaqpPFFpGmAOHbiuxDBJT9bTq1i/kb+0gilCXTasKwKqFn
cHSv3oeEE+qgBIWzZ3WsiaSnu6Ry15I+E+kM2a7XHG6r92vw3VHgczbmD7EHphoc
P+W6XzWbh501t8PUxJYMvcR2dYlHAGs+XyCyXgkL12ouZvGyzABnTREurKfWibSM
sNKFzE6wGGjIUFBb9I1cpV6pTs7Lmx+hGncZhoo1FK7QDJ2yRlwefyNhZQARAQAB
zR5DU0lSVCBEYWhhbmEgPGNzaXJ0QGRhaGFuYS5pZD7CwY0EEwEIADcWIQQppQpl
HpNHKJsY8hm32K9caRKkqwUCaZv7hwUJBaOagAIbAwQLCQgHBRUICQoLBRYCAwEA
AAoJELfYr1xpEqSrkAYQAKyo63wwgSxC5+vG23b1CeV0O40Pk6bQf7HTCd+EreA5
xTnNcGc2VDFQ2oNJCmmGpWos4eUiIQCSfh9p0WiM5a57izuT4Uzsmp9w2bZYM0/Q
VHzjBUvyPEezw4Vaq2SuV4eWHMifXeFtDB070T6y4EaRpT33ccdyEk0ki8dsyedx
DpuN/wv1R/Rd9YxI+nYnljAukoTSasklHFtm3iPoQK53wJNHfABByA3lNQVbfuHpt
4/+ampVHUlFRW/gqQ82PPLEi0Vfz8Tl8XL5R7CuEUyXJfUZn/qRyHJ/zfVunyOfw
Alkg4vYoPdnf3NV52L4v+Dq9FnM/8Ym9sBr4mLAjX931KBiJCVSZNQ3nHP1rlL1C
zvGHF3eYuA5EtI9i8kleIZpO7OA9UV2BeheGzMrDht6QyrUKos6dqwTlaeIHMtEa
b8u8yf6PviOK9xEhzYfeBg29ljRXLPATh49ScXMpo1MXFpVWPeDYhFrOsJAPb50K
uM1mWzy1kMz4Y3GpmODfDtzlfgpIh6hfvrvRyUEeZuAKQt3EfPEXUonnoe4fSPFd
ZBhude70TeCwvPTIEy1pOvw+27sAAPYx8U4u1AufRVgJ3ObRVEKHqSznqnEMVT0T
Kp2Bnjd0UJjvORScu19Nb0A0AVWXEjhZxPaqpgX7uEyN94zQnoh5cgi5oOMaA/Fi
zsFNBGmb+4gBEADRsE8YvK1Avh+JLwjuBBZb8ppUKdYrvOFz5pi+BI/nU5Gj0DcH
lbpT+1xOt1T955hOSkaIbYm5xu9AVBZARlLRH33u8GoEvOK7W16BI6cLzUM/77B6
He5FO6Pq/P3Zw6VFtpQqkyH/R1zfajLF4aPpnmzfhrWmGJ5yelutwl4ANBHx4+Yb
8LM7Ayxx0UCOjHonVucdJA7rkeHRnFxK8lTFbhA8f1h7eEAPmcODWT6jP13bMZBh
nMmPVyZP5p12gy1CuFB1XXydx8zXsA3rJd01bScTFdSToCsS12G4/p8jNfFJZDT/
qBc92EHjnoiPbe6R7VsFE126ihpE5l6aFTJJ2fzJWjuNeS8OUVHXefGrViU+GFQe
0NkxH4UcpJ3BpXyrbArHtQFHKYOxdX+TOGRXXKV7lxKoDdIhYWlpC2uSsgnmUanH
rhXso2D+wgmk8sIHBzvDVd4QK4fx6fQB3zoyFFQJwxMlAjmTa8MaLT/s+aAJgnSk
ijkUhSgQv9e+PQ2qW5rCGJA9uRL2AbV9fHRgMUfL37KzfhMVbFOHqf9nDbh7u42X
PKgsRz2g4Iq0zGBE+2APDAO7ghwGMzw6FiAfQ8T3DWJxMBDn9WWKgSzn8rlYka0+
3tXwygyfcn1rYvhzmN3bZGhgDt7htLlx1gM0jc1EA95yTyxQgx9aC+fR2QARAQAB
wsF8BBgBCAAmFiEEKaUKZR6TRyibGPIZt9ivXGkSpKsFAmmb+4kFCQWjmoACGwwA
CgkQt9ivXGkSpKvcfQ/+IvOT2LU27odfXGATWWEO2cHAXvjnlUeT+yClwWhDtrfO

Bm11uTVSfbtpBGcTUexeYYCCMrZ/EBynCMoQ+rwZEULkDEaWVNqmSG3htuTOSVBb
/BHOm/bMosk6/iiIR+yMrPUliugQ/zpmvvyAzhorhlx8NLwkVgs+2zQ0MIIKGSyK
hcGSTRk21qXXcI0kD4Ka4TwihDap6n4k1DAGBjxJyragniOilN6gUStFPlaAlwDw
K21wREEkLSxUjiB2WVnbWbGGM5/75iNFhV0ZqZ7Xp1z5jZhBdJ6NYexz0mbywxuf
1aNCUSifVVk/KQpXZ10l6iLaPSPUWC+8lrtPFloqiqmGn58RQt+RORMLNunVHGah
PlEyHgBtATMfmyJEyIe6Uh7bWaHtDshQ+Jz0qPoR16dPefKPaomBfA24fUxbZXeF
JcCtQdf9SPkW38AWNb58Ob27tBDExOEde1iqGXAT5YtMhqJfhYUz71KLS10BiITK
SxZbY6zGziS4QrpKxA2sU9Z97WMTh4l6lSh1wB/YIpzR8Vh86hF99syHUp1D6kZo
ywPr/DQoYoGb98UhLklriaiS0Ge+YZ6iKCzZGrSA9wagT0k8mWrDQGr9l/oyFne7
CoNAzqEsGSsJmCKMycW8/Ci58K/oWLcS6FZ/z/K2T19B/RRIyDgjpxPUDJMsAr8=
=jRSJ

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

File PGP key ini tersedia pada:

https://dahana.id

2.9. Anggota Tim

Ketua DAHANA-CSIRT adalah Senior Manager Sistem Teknologi Informasi – PT DAHANA.
Yang termasuk anggota Tim adalah beberapa pejabat struktural di lingkungan Bagian Teknologi Informasi PT DAHANA

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak *NAMA-CSIRT*

Metode yang disarankan untuk menghubungi *Dahana-CSIRT* adalah melalui *e-mail* pada alamat csirt@dahana.id atau melalui nomor telepon yang tercantum pada Informasi Data/Kontak. Pada hari Senin-Jumat pada pukul 08.00-17.00 WIB dan jika terdapat hal-hal yang mendesak di luar jam tersebut dapat dilakukan penanganan.

3. Mengenai CSIRT PT DAHANA

3.1. Visi

3.2. Terwujudnya ketahanan siber yang handal di PT DAHANA.

3.3. Misi

Misi dari DAHANA-CSIRT, yaitu :

a. Memberikan keamanan dalam layanan teknologi informasi untuk menunjang operasional bisnis
b. Memberikan pemahaman dengan mengkoordinasikan pada pihak karyawan atau konstituen terkait ketahan siber pada jaringan yang digunakan.
c. Mengidentifikasi, menganalisa dan evaluasi setiap insiden yang terjadi pada ketahanan siber

3.4. Konstituen

Konstituen dari DAHANA-CSIRT adalah seluruh karyawan PT DAHANA yang menggunakan layanan teknologi informasi yang berjalan dalam infrastruktur teknologi informasi milik PT DAHANA

3.5. Sponsorship dan/atau Afiliasi

DAHANA-CSIRT merupakan bagian dari PT DAHANA sehingga seluruh pembiayaan bersumber dari anggaran Perusahaan

3.6. Otoritas

DAHANA-CSIRT merespon, menanggulangi dan mitigasi insiden siber konstituen maupun organisasi di PT DAHANA.

4. Kebijakan – Kebijakan

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

DAHANA-CSIRT memiliki otoritas untuk menangani insiden yaitu :

a. Web Defacement;
b. DDOS;
c. Malware;
d. Phising;

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa DAHANA-CSIRT Indonesia 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 DAHANA-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh DAHANA-CSIRT berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh konstituen.

5.1.2. Penanganan Insiden Siber

Layanan ini diberikan berupa kegiatan menerima, menanggapi, dan menganalisis Insiden Siber.

5.2. Layanan Tambahan

Layanan tambahan dari *DAHANA-CSIRT* yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berupa koordinasi, analisis dan rekomendasi teknis dalam rangka penguatan aspek kendali keamanan (security control) baik dalam lingkup teknis ataupun non-teknis (Policy/Governance).

Secara umum penanganan ini dibagi menjadi :

1. Pelaporan kerawanan yang bersifat sewaktu oleh pemilik/penyelenggara sistem elektronik milik konstituen.
2. Layanan penanganan kerawanan sebagai tindak lanjut dari kegiatan audit atau vulnerability assessment

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan berupa penyampaian kepada konstituen terkait ancaman terhadap Sistem Elktronik yang dapat muncul akibat perkembangan teknologi, politik, ekonomi, dan perkembangan lainnya.

5.2.3. Pendeteksian Serangan

Tim DAHANA-CSIRT memiliki beberapa sistem untuk mendeteksi apakah sistem pada perusahaan yang bersangkutan dengan stakeholder aman atau memiliki risiko, sehingga dapat dilakukan penanggulangan sedini mungkin.

5.2.4. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Tim DAHANA-CSIRT melakukan webinar mengenai isu sistem keamanan informasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@dahana.id dengan melampirkan Formulir Aduan Insiden Siber yang sekurang-kurangnya memuat :

a. Identitas Pelapor;
b. Tipe Laporan;
c. Waktu Terjadinya Insiden;
d. Tipe Insiden;
e. Deskripsi Insiden disertai Bukti (screenshoot, domain name, URL, email dll).
f. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

1. Terkait penanganan jenis malware tergantung dari ketersediaan tools yang dimiliki.

2. DAHANA-CSIRT hanya menyediakan sarana komunikasi melalui kanal yang tercantum pada dokumen RFC-2350, kami tidak bertanggung jawab atas komunikasi yang mengatasnamakan DAHANA-CSIRT melalui kanal lain selain yang disebutkan.