RFC 2350 *DWARAPALA CSIRT*

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal Agustus 2025.

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://dwarapala.id/csirt/RFC_2350_DWARAPALA_v.01.pdf

1.4. Keaslian Dokumen

Dokumen ini telah ditanda tangani secara elektronik oleh Ketua DWARAPALA-CSIRT.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 *DWARAPALA CSIRT*;
Versi : 1.0;
Tanggal Publikasi : *12 Agustus 2025*;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

PT. Proteksi Siber Global (Dwarapala) – Computer Security Incident Response Team
Disingkat : *DWARAPALA CSIRT*.

2.2. Alamat

Talavera Office Park Lt 18, Jl. TB Simatupang No. 23, Cilandak Barat, Cilandak, Jakarta Selatan, Jakarta 12430.

2.3. Zona Waktu

Indonesia (GMT+7)

2.4. Nomor Telepon

(+62) 85183380156

2.5. Nomor Fax

N/A

2.6. Telekomunikasi Lain

N/A.

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

csirt@dwarapala.co.id

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

---

Bits : 4096
ID : 0xD3A0DDF82BDDA92E

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

xsFNBGhmPlwBEADVlNhHP8F0PshdR8QfQl/8UQtHMEEzxwuo7+osgO099zHoiX8m
YqoeKM19cwQeF+VWmxttp8NbyByYZLPYQBMuIHQRaMbXTVdA+ggCa9UOb2mlQmKh
SJvGe0FmIz6UFNcqrzEjHn0BBQaiGmeNL9xUHp0n9kVsiksRcUsptYK33+RPXGVD
V8wb5fPSbVG39jlEYybVG0RLOCpeG+hMDF1jMW71RDELR/TpSgw7Y0Or0ONTVdlU
B3jddWOa9jhFe6udy5/O/kJksQToMQ7XUwzDZjxPASUO41a30XVZ+Q1xIgO8/PAP
cp6ueZPH5v7iwKtalsXpivTKTvqd0ckEIneiCDZjUNBa9sGJuCUDfEC8hG2Jnnbl
bKcvl9VoaxcrfGKGOp/mkIB8FoP/wVRfkYeflq9/JPOReihw4oygNWj+Gm4Eag8v
gUAXUQ4ReY0n1R6lHErGNWZlKcu802Nz4A4BJrt/UGaP6rWEAu5glZEPkkUszWTf
au8BgsuRb4jw7805M8Rqvm0uNXuN0WC0rwSitbuzyA/88qlEfmc2pSSUrx6FAoo8
qiml6bxvYj8KZTe/6d+AzxGGMTVfR4Npjg7erDKEAAGgv8Fj3j33uSdJAb7p7RfH
a2Ep/H0jnsFkkmkTiXQWC8095zRtp2wSDpuimCJxB1IiQKjPJtxNmxaMvQARAQAB
zSdDU0lSVCBEd2FyYXBhbGEgPGNzaXJ0QGR3YXJhcGFsYS5jby5pZD7CwY0EEwEI
ADcWIQTj7RBvUcwOs26P96LToN34K92pLgUCaGY+XAUJBaOagAIbAwQLCQgHBRUI
CQoLBRYCAwEAAAoJENOg3fgr3aku4vYQANIb5jsWyRYthDqRxvkr0Rb6+e6YtQrJ
p1Eg/gfmj4M+dxhFNIbrLFQBjvG+1/xCTrc3TlrkzF/cGS7uBjEDsB06Lsqct9v2
R1mN/D8CdLKEPSwWZuP4Nlxy9BxF1NB7O2SJVXOxBnCIX1O7oH6eAuuvNa8Tuf2A
lM6jKitPtztx581QxWZUSrD1a/dY8BlgZewHJ4WJ/IbngzxgE8du7ZOcKNLl+nOI
tPmKQdKrjyNudG+9oCESzDnsPxlCAVv0OSCPar6chca1qVkNZdzi+C0JRzR3ZeY+
lqC/CllsI21o0U071050GdOyDDUXpeVN9faAsXTvCP/Tnz261rTYO7IkkKbCsiWB
TmrBHg2UFUDuPGvxQ3WCnYB1TpsRWNepwC2rWhMsFyV7SK5vGag9GzzVkayh+e47
U/gMYZqSEtTZKd5l3OP7Y1u996LY7GKlBU39IrJT+FDFtYYEJx0WHIb+UAFWn0GF
u5OMq+BXemm4S8Ie6JaoOd01FMCXeGgjocYPORQ4ZApOwwYfpfG9/m+tkZeGCZ8i
aNHrJpKRfb5tvEu59WFRuJLfYrjaTLq1YpD7X1cD0aGBIlcyhMZ+35sp1It+WitA
AE1e7oEzzN2nSpm1vFwblmtaZitlUJL8IlzznXrDUR5dRpnztzyyZjeJZSWWAWhP
JsfyRymIj1Z3zsFNBGhmPlwBEADhJV6ahUykQB8MTPxmBFCcecoi/UAtTlbbP6iG
dz22JPbjjdpdW/HekFZw9uS1/G1kAZYJOJO0IyJoN1CM9tOUPf16DtlXO1aqqORW
jntlPtTBYav+MZ5+fOBmJFy7O/pIi59hBQHLXvSPFVpDVcwZw34E1dIF0ot6iTzo
DymNElual8V6Ua7kcfvgFpTryOFICDavFcsefsJZWov9QW79QMXxTe/8UMrkg0e2
DXPTM9FbOcYEwks8VoGHZdcqBkepSGzfAvA7Ab4qS0cptoEttrDMzJ/FXCpbfq9u
5cMDQSM0l3dH6KuFMn3auQwLZs6gQ+YJWWJvMT/D3woXzBPQzNMMCCLXD+pZdVCn
a3oua+006o+kbArDv41FAWw6hJAgKdpBwmd7/htMzAG1FykUFv/2wBbjY29FqAld
6PNs3FP8E0SYckZ2AzlB9SPlEwLRZ/RzXMgDkAI3xaCApTbCs7FXaoIDqPAd3FR2
fOPQI0SrXGNzujJSPyVKe8eifN6fpQPf55fuNOYcKj1Lz45RPGSeBn/RXIp0N01A
xfA1rTCxpFvMxp6MxADNCVnt9gmnA+LITBuVLS7NpQT6tpqWmhA7OlphT41BzvlW

6tcBukR06li/b2jkmolMyH1qq1SkbpdiDDbxrrAaZurzH4fEAjBE4TC3JmM1hsWC
R8w6TwARAQABwsF8BBgBCAAmFiEE4+0Qb1HMDrNuj/ei06Dd+CvdqS4FAmhmPl0F
CQWjmoACGwwACgkQ06Dd+CvdqS62PBAAwY30B4sFteRKNv03/zRG85JurLpv33v4
j1jE15/nCCwPkvW6QfKi4UCAb00u3gjsl3ZYnXtLmld3+EW9sZeJ19WCPZDyE82B
aHKHopev98ZjaqBbXxsa9itBEe/X4IaRnzh2oSaR3fJ5noDe2kUKOkSOXVXa8vLq
A8Ptb41uGxwbqrs9Judy2ZeXZKKrWwkQ4uc9u7CDkugcAkPUbgr0snCZxa+kaMB5
hjeLXznZwlRxPwGIyb6ChCBpzwUxoEf1SZmNNaDh6zUjExi2OzcSFeptQ1kpsyKW
6xXTdRqaitjNEbS8DGSzEbAOSffjxzkpBhI2pDUw7sbWJvFLPda/8o3/KFc/MZ1H
ksSBBA8dXOFOtDd+yeH/aUENapGnJ91Jiq+xieAHtC6zTUUv5siKWTCDIXBo97bX
0Maakuj6m/F21a9diwF6/3ergVcozLw+p6KAPZF2uvsla/a6XUkOlSnwbV/RPHGz
MndsTLpFzL4YRL3N8nzZZ+sF8/ssHSWQ2MXjKa0znlj+oqb1ZOGO5Bu0GWq+x5jx
MN+yY1OGHoAJCB//G0bcSw3Ucka5clyJHDeHA0wLRFBxoL3b/sORxOY62VNz+1AQ
fLTIX2z1gNB3eyv0L5JHxIQLrSC8Rdcukc+yeBUzGBoKe4YiqogYs752OWJxQ8EU
I9knHU8y9Bo=
=3ZLJ
-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada:
https://dwarapala.id/csirt/DWARAPALA_CSIRT_public_key.asc

2.9. Anggota Tim

Ketua *DWARAPALA CSIRT* adalah Manajer Senior / Executive
Yang termasuk anggota tim adalah : seluruh personel tim Security Operations Center (SOC) Dwarapala, termasuk analis keamanan, tim monitoring, serta personel pendukung teknis yang bertanggung jawab dalam penanganan insiden keamanan

2.10. Informasi/Data lain

N/A.

2.11. Catatan-catatan pada Kontak *DWARAPALA CSIRT*

Metode yang disarankan untuk menghubungi *DWARAPALA CSIRT* adalah melalui *e-mail* pada alamat csirt@dwarapala.co.id atau melalui nomor telepon yang tercantum pada Informasi Data/Kontak. Tim CSIRT dapat dihubungi mulai Senin – Jumat (07:30 – 16:30).

3. Mengenai *DWARAPALA CSIRT*

3.1. Visi

Visi *DWARAPALA CSIRT* adalah menjadi komponen utama untuk tercapainya Visi Perusahaan dengan meningkatkan ketahanan siber.

3.2. Misi

Perwujudan visi sebagaimana dituangkan di atas akan dicapai melalui upaya- upaya yang terkandung dalam misi *DWARAPALA CSIRT*, yaitu :

a. Mengkoordinasikan dan mengolaborasikan layanan keamanan siber di lingkungan Perusahaan dan pemangku kepentingan.
b. Membangun kemampuan dan kapasitas sumber daya keamanan.

c. Membangun kerja sama dalam rangka penanggulangan dan pemulihan insiden keamanan siber

3.3. Konstituen

Konstituen *DWARAPALA CSIRT* mencakup seluruh pengguna yang menggunakan layanan keamanan siber yang disediakan oleh grup perusahaan Spentera, termasuk:

- Seluruh karyawan tetap dan kontrak yang bekerja di bawah naungan Spentera Group,
- Serta anak perusahaan, yaitu:
  - PT Proteksi Siber Global (Dwarapala)
  - PT Hacktrace Siber Indonesia (Hacktrace)

3.4. Sponsorship dan/atau Afiliasi

Pendanaan *DWARAPALA CSIRT* bersumber dari anggaran Perusahaan secara mandiri.

3.5. Otoritas

DWARAPALA CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi, dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber pada sektor layanan keamanan siber dan teknologi informasi di lingkungan Spentera Group, termasuk anak perusahaan PT Proteksi Siber Global (Dwarapala) dan PT Hacktrace Siber Indonesia (HSI).

4. Kebijakan – Kebijakan

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

DWARAPALA CSIRT memiliki otoritas untuk menangani insiden yaitu :

a. Web Defacement
b. Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks
c. Malware
d. Ransomware
e. Phishing
f. Application Attacks
g. Data Breach

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa *DWARAPALA 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 *DWARAPALA CSIRT* yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh *DWARAPALA 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

Menangani insiden keamanan informasi yang memiliki impact dan severity tinggi atau diatasnya, yang dapat menimbulkan gangguan pada kerahasiaan (confidentiality), integritas (integrity), dan/atau ketersediaan (availability) sistem informasi yang dimiliki oleh perusahaan.

5.1.3. Cyber Defense

Kami merancang, menerapkan, dan mengkonfigurasi langkah-langkah keamanan yang efektif untuk melindungi sistem dan data Anda, seperti firewall, sistem deteksi intrusi, dan enkripsi

5.1.4. Managed Security

Layanan Keamanan Terkelola (MSS) dirancang untuk meningkatkan posisi keamanan organisasi Anda dan melindungi dari ancaman yang muncul.

5.1.5. Security Operation Center

Pemantauan terus menerus sangat penting untuk mengidentifikasi dan merespons ancaman yang muncul secara real-time. Kami menawarkan layanan Pemantauan Keamanan yang canggih, menggabungkan teknologi mutakhir dengan analisis ahli untuk memberikan perlindungan yang komprehensif bagi organisasi Anda.

5.2. Layanan Tambahan

Layanan tambahan dari *DWARAPALA CSIRT* yaitu :

5.2.1. Pendeteksian Serangan

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

5.2.2. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Tim *DWARAPALA CSIRT* melakukan webinar mengenai isu sistem keamanan informasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@dwarapala.co.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*

Tim *DWARAPALA CSIRT* memiliki beberapa tools untuk menghindari malware antara lain:

a. Menentukan asesmen tingkat keamanan informasi pada proses bisnis yang sedang atau yang akan berlangsung;
b. Melakukan asesmen tingkat keamanan sistem informasi yang dibuat secara sendiri (in-house), atau disewa/dibeli ke pihak ketiga;
c. Melakukan pengawasan serta intervensi aktif terhadap operasional sistem informasi dalam rangka pemenuhan ketahanan dan keandalan siber yang menunjang tujuan bisnis;
d. Merencanakan, membuat dan mengoperasikan rancang bangun mekanisme pertahanan berlapis siber (cyber defense-in-depth);
e. Melaksanakan program kesadaran keamanan siber bersama stakeholder terkait
f. Memiliki otoritas penuh untuk melaksanakan koordinasi dan intervensi internal dan eksternal, akses terhadap data dan sistem dalam hal penanganan insiden siber Anti – Malware.