RFC 2350 *PERISAI-CSIRT*

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 02 September 2024.

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://csirt.peris.ai/rfc-2350 (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 PERISAI-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: *23 Januari 2025;*
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

PT. Perisai Sistem Keamanan – Computer Security Incident Response Team
Disingkat : PERISAI-CSIRT.

2.2. Alamat

Jl. Tebet Barat Dalam IV No.6, Tebet Bar., Kec. Tebet, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12810

2.3. Zona Waktu

Indonesia (GMT+7)

2.4. Nomor Telepon

(+62) 898-8995-918

2.5. Nomor Fax

N/A.

2.6. Telekomunikasi Lain

N/A.

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

csirt[at]peris.ai

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

Bits: 4096
Key Fingerprint: DEF8 C376 8F5F 52F7 6B3C 4A1F 871C 98E1 CFB6 E3F2
Key ID: 871C98E1CFB6E3F2

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

xsFNBGbWvHkBEAD069965BnlcE0uaz9S20kjbLwglDDbkidrqM4NsCarWz43
H+F2scyhVsJ7lsju6W3L8JBTxxDoWdn2X/Ehxj4TLwj4n0eKWUzLXO90+e8t
BgrR4BPUegq/Fv7zzR8C3XYNxWC5YZfhsUbpSQ5RNgBxRQortdNI7I9y4sUr
mQfjlwCK+YeNzToptHDso+XpuvsqYJNKOh4gffkvo6+9QWm1fLeXXtj36NUR
4ALEDkW8EUZbtCsJehj43oM3B9VkIJ5NxbmpLEdd4XADUUpZJaL8mS6rmaCY
po0KYx5nbBR1o9W6ZMaWSq3Eg9ucGg1+t438tT/BAwzlzaiZuLmYP3205Kuc
Q1jx2Z9Cs8OFDINLcKxw6yKmXaAHa57up6g8cOPTpqQyoiqt/DFvpbpBOlpx
/A4yD6hhrRwJISVO3FheQat2IRPiezRt/YENzNz9NqXgdTkE3929aqlfOxTR
FAk2IT7oOh+zZAkwbKt4jHDqqbrKLI8mZdGaiJ0iMiqQsAZjAkHg/vbm6cmr
Kr6FM5P37FkgQq/iXQilCqbaJSYCZn1GBqYXkuB++LZ9sqVYAupNYOd55yU4
1gjZkrl28Ri8TIJSVFZxRWD2tY+SNEX9njBTP/XnpCpRsirQtPF1IBsFz0s7
3l/3jl/BXH1fRolDY23wVuv0pfMETeb8CGvTCwARAQABzR5DU0lSVCBQZXJp
c2FpIDxjc2lydEBwZXJpcy5haT7CwYoEEAEIAD4FgmbWvHkECwkHCAmQhxyY
4c+24/IDFQgKBBYAAgECGQECmwMCHgEWIQTe+MN2j19S92s8Sh+HHJjhz7bj
8gAAsQAQAPN6dHezs/81HQtKFJqWNQxUMaXp6mooA52mqLYEqXXjg/Qp03mR
VLYHouhEo6C6TMtOU9WOFQj6nhPROQ96tNN/T5mCb2Nzhy8N9kCeHjkxLirC
GYOSI4qMce4W4dGjKOo3GdFwer+bLiI8avZciR06T7qW4MmRNyPvYQhNEUYX
GuR+P938J1lomCTqUIkiUG3AlMeNiLYWRjW7djCesAUm2RFkYYbAYy8l2MV1
m2YnDeX5KVz0/XcvWFAEZTg+WLY6Ou/SXDzFQz9RrysCy3QcPt5Ni05gGx9A
k2YlKr9ltgH5hISElrBzfbvguBlGHl4+CB9OHIlpXJnGTv7Mgl7YQre5Sv5t
zya9Vxycf5bksitQ0CDpXlaiggwh7TwHKNcPKhiIxwGmWTqW+2vDj9xd9H8x
3oCfeY+LdSs2LrNIKTKEHmbwvW2ENoy5xSkiOKyl4jsjIab7DaG8W8bmib02
ssNG0QNKuB3G133MNFMlQy8E/dnR7TjCsay5R7z0mdi6piSRgXEdaRZKXOif
E+/dtT6DaPs4cnv28+VU3NNoFFKd5y1Skk8T4JL/yt7CXvN73SGWNZVzXu7Z
lB/M3Y6c9g0kaWIl64rqcVEylbkyBkW0jclEOto2stuXkSyUiF+tbLnsfCwv
bcWY3dvZvRLIuFDJr6oxiC2APefwhjWmzsFNBGbWvHkBEAC4ViNmut1Gf2//
tpxPm8rR4vBXkIFHngHIRyJ+HFaL+gHrc3HrkJaeTqhSuChVS+Ko5Nj1vNQE
BG8stvQjjSW6zAV5upDs8JKhjQzPfUtvXbA8S6mjjG3aSZg2c6pNw+tW2aRY
88rAXPVlkv5t+47lrkVGJ5ufiqM+tWxEHvH+PJmOGBEBLahezJB57PalKVLu
txW/3yFfcGo9/7vEy2oULe3K6WBTz2fhHwxg6G6G5tDi+PcfOHWzdHjG32PC

iDb/G7IMnQsvrNf0pZlwOGj4BzjVPUC1hP9naNE/icscbUFu788uZ8KX/i3o
+O1ENQzcwBEyr7ooK4BYjpCQ0ZWGBwG72Jo8rlhbdIG+o3GaFi5pi9d9ZwKC
p/nLjQ/4LhdvQGvC31zqstt3MlP5QMc0t9XdtHXSFZSHKGwGn4cZ/jy1iG3a
LA4hVw75xqdZjz6cVn9p+pXZfcQMvpuN/nUddljRbvX3D6ax1pdZLAq1Ub7h
QGrcnxp0iQnyU8RJB/aB9BMDCHAQ82gCMm1vlXjyzQv2G8bUvKOrYEShctVk
zoWnI6bkYU/bYrONQHrPyZRGIc31CJb33tqI0AKB3CyodnqoY9nww9dYRGd+
q46JlaT64aR6MaSyGwaIcGUy/C2hRBeWlDpI8FxxcWlKI9aBUYxbZ77pwoVw
pnsI8tT6bQARAQABwsF2BBgBCAAqBYJm1rx5CZCHHJjhz7bj8gKbDBYhBN74
w3aPX1L3azxKH4ccmOHPtuPyAAD0qQ//Q8sFkQryE7boJF9mmK6g/BE4hA2R
EPoz3MxR8T4xaGlw0/8BaG6sCfjQyMc3CqIPQuCpU99mePOyjcwTX4UlRPEM
y0fQSRxh2PTABp7ReS7bh2UoFmDwOhTs0lklfMibKhK4fOYqjpHZId82ZDdc
lrKDqD5ux62MLdq4EJcjWeIUmD/edAp+DPHKQ/s8EHrxidKXr0K0Sl3dCGW9
616EdkgkJHTZSmNzBTP4sHtZ7WbqPtK+uIi0T+IesgyE8aMcGqO8OfJdZgvG
RH9NBm4dciRr4fgL+XUlWiVmsVGtHu/KaKh4vbAOIV3b190aTrdOCONQlajc
ulQ6cU5ZEha3Ev8cFiZARAwlf/AsN4N0KLHm/65MedTsJ4aPW+X3nXxGoSS9
t7FpY9l46PstCE/iVjkoz/5iA4njeI2N3hva+z/l/0zZjrk5qKwP9T4Nb7E1
EjkjDuumxrCgpm29JZ1XzKOi21FvP4V9RF01xm2Mr40YL8cfmMjP0611ByOA
7NVcathxgassOZ0ksD2FcqU+4eI3eFQxIgK+V0+fesm9eSgePTyHUUU6UxON
45vJvlubsqb6AfQGYM1ciPtWmbFQW2fFBdaQgoZDDRx7s0uYD8bPHlloIVA1
tozYPQ2tZBk97+5hFexFtrH58j0Gs6YJhxZg9joYI6lvTpdHXaPAVIQ=
=mDm0

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

2.9. Anggota Tim

Ketua PERISAI-CSIRT adalah CHIEF INFORMATION SECURITY PERISAI
Yang termasuk anggota tim adalah SELURUH TIM SECURITY PERISAI

2.10. Informasi/Data lain

N/A.

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

Metode yang disarankan untuk menghubungi PERISAI-CSIRT adalah melalui *e-mail* pada alamat csirt@peris.ai atau melalui nomor telepon yang tercantum pada Informasi Data/Kontak. Pada hari Senin-Jumat pada pukul 09.00-18.00 WIB dan jika terdapat hal-hal yang mendesak di luar jam tersebut dapat dilakukan penanganan.

3. Mengenai *PERISAI-CSIRT*

3.1. Visi

Visi PERISAI-CSIRT adalah menjadi komponen utama untuk tercapainya Visi Perusahaan dengan meningkatkan ketahanan siber di sektor industry.

3.2. Misi

PERISAI-CSIRT berkomitmen untuk menyediakan dan mengoptimalkan sumber daya pertahanan siber melalui proses pembelajaran dan peningkatan kualitas yang berkelanjutan.

3.3. Konstituen

Konstituen PERISAI-CSIRT meliputi seluruh pengguna yang menggunakan layanan PERISAI CYBERSECURITY, meliputi karyawan dan anak perusahaan, yaitu PT Perisai Sistem Keamanan

3.4. Sponsorship dan/atau Afiliasi

Pendanaan PERISAI-CSIRT bersumber dari anggaran perusahaan.

3.5. Otoritas

Berdasarkan Kebijakan Pengelolaan Sistem dan Teknologi Informasi dan Kebijakan Pengelolaan Keamanan Informasi, PERISAI-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi, dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber yang terjadi di konstituen PT Perisai Sistem Keamanan.

4. Kebijakan – Kebijakan

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

PERISAI-CSIRT memiliki otoritas untuk menangani insiden yaitu :

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

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

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

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa PERISAI-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 PERISAI-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh PERISAI-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 PERISAI-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. Penanganan Artefak Digital

Layanan yang diberikan kepada konsitituen ini berfokus pada pengelolaan, analisis, penyimpanan, dan pengolahan data digital, khususnya dalam konteks forensik digital, keamanan siber, atau manajemen data.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

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

5.2.4. Pendeteksian Serangan

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

5.2.5. Analisis Risiko Keamanan Siber

Tim PERISAI-CSIRT memiliki beberapa proses sistematis untuk mengidentifikasi, menilai, dan mengelola risiko yang terkait dengan keamanan digital organisasi, yang bertujuan untuk melindungi aset digital organisasi, seperti data, sistem, dan jaringan, dari ancaman keamanan siber.

5.2.6. Konsultasi terkait kesiapan penanganan insiden siber

PERISAI-CSIRT memiliki konstituen yaitu pegawai PT Perisai Sistem Keamanan yang menggunakan layanan teknologi informasi yang berjalan dalam infrastruktur teknologi informasi milik PT Perisai Sistem Keamanan Serta anak perusahaan PT Perisai Sistem Keamanan.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

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

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@peris.ai 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

Jakarta, 30 Januari 2025

Feri Harjulianto
Ketua PERISAI-CSIRT