RFC 2350 CSIRT UKPETRA

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Pembaruan Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 18 Juli 2023.

1.2. Daftar Distribusi untuk Pemberitahuan

Badan Siber dan Sandi Negara

1.3. Lokasi di Mana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.petra.ac.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 CSIRT UKPETRA;
Versi : 1.0;
Tanggal Publikasi : 18 Juli 2023;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team Universitas Kristen Petra
Disingkat: CSIRT UKPETRA.

2.2. Alamat

Universitas Kristen Petra Jl. Siwalankerto No.121-131, Siwalankerto, Kec. Wonocolo, Kota SBY, Jawa Timur 60236

2.3. Zona Waktu

Surabaya (GMT+07:00)

2.4. Nomor Telepon

031-2983312

2.5. Nomor Fax

031-8417658

2.6. Telekomunikasi Lain

Tidak ada

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

csirt@petra.ac.id

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

```
    Bits             : 3072
    ID               : 5AC6 452E EC9C 33B5
Key Fingerprint      : 65140FFC469EB67A105442595AC6452EEC9C33B5
```


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

mDMEZNmleRYJKwYBBAHaRw8BAQdAl/IvwiKpxvE0DfdknAcRmDk+CCHfFbwAxr1t

F15oo/u0IUNTSVJUIFVLUEVUUkEgPGNzaXJ0QHBldHJhLmFjLmlkPoiTBBMWCgA7

AhsDBQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAheAFiEEZRQP/EaetnoQVEJZWsZF

LuycM7UFAmTZpY0ACgkQWsZFLuycM7UvkwD/fCJJpatqo0OLhWg6/6fiuEGBMk/F

v7ci6OALtrMZxIcA/RY1b99oS7k4MDmdKtev3Q3yfpuFmA0JJQOBIqZ15bULuDgE

ZNmleRIKKwYBBAGXVQEFAQEHQB263IoyQxauJ4umqTrQVe2JPiEahJ8hksrac7tn

40YeAwEIB4h4BBgWCgAgAhsMFiEEZRQP/EaetnoQVEJZWsZFLuycM7UFAmTZpY0A

CgkQWsZFLuycM7XBkAD/Tf/oBn88SfdJAo/C5sBo7RDsStVTH0v0tr05z6wYgT0A

+QGbAuWD46rff7xxCc+jSaT+r+bVpvpBzhtvpxc9hlEJ

=rChf

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

File PGP *key* ini tersedia pada :
https://csirt.petra.ac.id/publickey.asc

2.9. Anggota Tim

Ketua CSIRT UKPETRA adalah Kepala Pusat Teknologi Informasi & Komunikasi (PTIK). Anggota tim terdiri dari seluruh staf Pusat Pengembangan Sistem Informasi & Bidang Infrastruktur & Perangkat Teknologi Informasi PTIK.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak CSIRT UKPETRA

Metode yang disarankan untuk menghubungi CSIRT UKPETRA adalah melalui *e-mail* pada alamat csirt@petra.ac.id atau datang ke Gedung W LT.4 UK Petra pada hari kerja pukul 07.30 - 15.30.

3. Mengenai CSIRT UKPETRA

3.1. Visi

Visi CSIRT UKPETRA: Menghadirkan ketahanan siber yang handal dan profesional menopang UK Petra menjadi universitas Kristen kelas dunia.

3.2. Misi

Misi dari CSIRT UKPETRA, yaitu :

a. Mengidentifikasi kerentanan keamanan pengolahan sistem dan teknologi informasi & komunikasi (TIK) secara menyeluruh
b. Meningkatkan awareness aspek keamanan kepada seluruh Satuan Unit Kerja UKPETRA
c. Meningkatkan mutu layanan TIK Pendidikan dari ancaman siber.
d. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber pada sektor pendidikan baik internal dan eksternal
e. Mengembangkan kemampuan ketahanan siber bagi sumberdaya tim (people, process & technology) dengan prinsip menegakan etika dan profesionalisme.

3.3. Konstituen

Konstituen CSIRT UKPETRA meliputi Seluruh satuan unit kerja UKPETRA

3.4. Sponsorship dan/atau Afiliasi

Sponsorship dan/atau Afiliasi CSIRT UKPETRA sehingga seluruh pembiayaan bersumber dari anggaran instansi UKPETRA

3.5. Otoritas

CSIRT UKPETRA memiliki otoritas untuk menangani insiden yaitu:

- Peretasan infrastruktur jaringan dan server
- Web defacement
- DoS & DDoS
- Malware
- Phishing
- Pembajakan akun UK Petra
- Akses ilegal
- Spam

4. Kebijakan – Kebijakan

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

CSIRT UKPETRA melayani penanganan insiden siber dengan jenis berikut :

a. Web defacement
b. DoS / DDoS
c. Malware
d. Phising
e. Pembajakan akun UK Petra
f. Akses ilegal
g. Spam

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi / Data

CSIRT UKPETRA akan melakukan kerja sama dan berbagi informasi dengan CSIRT dari Kementerian dan atau Lembaga lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT UKPETRA akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa, CSIRT UKPETRA dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT UKPETRA yang menjadi prioritas yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

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

5.1.2. Penanganan Insiden Siber dan Pemulihan Insiden

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

5.1.3. Penanganan Kerawanan

Layanan ini diberikan oleh CSIRT UKPETRA berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (*hardening*), CSIRT UKPETRA memberikan informasi statistik terkait layanan ini. Namum, 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. Penanganan Artefak

Layanan ini diberikan oleh CSIRT UKPETRA berupa penanganan artefak dalam rangka pemulihan sistem elektronik terdampak ataupun dukungan investigasi. CSIRT UKPETRA memberikan informasi statistik terkait layanan ini.

5.2. Layanan Tambahan Proaktif

Layanan tambahan dari CSIRT UKPETRA bersifat proaktif yaitu:

5.2.1. Pemberitahuan Hasil Pengamatan Terkait Dengan Ancaman Baru

Layanan ini diberikan oleh CSIRT UKPETRA berupa hasil dari sistem deteksi dini sistem monitoring keamanan. CSIRT UKPETRA memberikan informasi statistik terkait layanan ini.

5.2.2. Layanan Security Assessment

Layanan ini diberikan oleh CSIRT UKPETRA berupa identifikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan. CSIRT UKPETRA memberikan informasi statistik terkait layanan ini.

5.2.3. Layanan Security Audit

Layanan ini diberikan oleh CSIRT UKPETRA berupa penilaian keamanan informasi. CSIRT UKPETRA memberikan informasi statistik terkait layanan ini.

5.2.4. Layanan Manajemen & Awareness

CSIRT UKPETRA meningkatkan kualitas keamanan melalui kegiatan:

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

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@petra.ac.id dan/atau melalui sistem tiketing https://csirt.petra.ac.id/tiket dengan melampirkan sekurang-kurangnya :

a. Informasi identitas pelapor
b. Bukti insiden berupa foto atau *screenshot* atau *log file* yang ditemukan
c. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

Terkait penanganan jenis malware tergantung dari ketersediaan tools yang dimiliki.