RFC 2350 Perhutani-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 26 Oktober 2022.

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 :
https://csirt.perhutani.co.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 Perhutani-CSIRT;
Versi : 1.0;
Tanggal Publikasi : 26 Oktober 2022;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Perum Perhutani - *Computer Security Incident Response Team*
Disingkat : Perhutani-CSIRT.

2.2. Alamat

Perum Perhutani
Jalan TB Simatupang No.22, Jati Padang, Pasar Minggu, Jakarta Selatan 12540

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021)7805730

2.5. Nomor Fax

(Tidak Ada)

2.6. Telekomunikasi Lain

(Tidak Ada)

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

csirt@perhutani.co.id

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

Bits : 4.096-bit RSA *(secret key available)*
ID : 2198A77C
Key Fingerprint : 1D0F14720D7802FFC06DB7F2B30A35C62198A77C

Blok PGP Public Key Misalnya :

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGNXn1sBEADAgjD3SO3xxXe99AO2AUwaAy8H+oqnCEgBxAnoehLKu6Cki72T
r+3M6iABurxsNQtLpXzun+AIsEMrIWpdPOTeM+VGCFVUltAVrxUex6ONjOx5m+4T
CLb/7rPHTfOlkA8vKy4ypHk88GPIsYki6e9qQPv5xdXZ8WLqvR5NAdV6QARikg/a
B9/gu860TVIfwDiqf94qnng2J+xr2Z4PJpEbAeYGnHw0f4tcOIKyBdqd4XEZwFyT
9AeOy7dDZClSn8MVUaZjcig97OKZyGE11bgL9nT6DDRvNo8+QVIlthN+Ebr24QtT
ZGSh7T0BowQV2/ZFzntg5PmqTVFPubM3u26sBcrxOljBztc9PUNy8DOAxowTGqHm
/QrxxsNh6PbGyfVSHmAwwROs84EXLVom0OtyFvhyKIc3RTL/m4fkXuNfH9UHW+ek
SF3uXj60j4XUutgZbRTcEImxi6ghdVkKfGynLn4Go4uuNwT6kf6geYIw4KhLrWE2
44jbtBsSUuCuyXyilrnMKhatt6yQYKZ0W65BO4YB/Y7AHA0zXSncIswqFUHEbdsG
2a3S/efrL7JleIekGe/6wiV1P3Wbb9tukzy1gGwgSlXacpAP389xxEzeLJIm0rfs
MpRrRHbYQa0JnHqYZCBwzuVfnwNkXVYAnguHHRHHKYcogJlOugvc1U/Y2QARAQAB
tCdQZXJodXRhbmkgQ1NJUlQgPGNzaXJ0QHBlcmh1dGFuaS5jby5pZD6JAlcEEwEI
AEEWIQQdDxRyDXgC/8Btt/KzCjXGIZinfAUCY1efWwIbAwUJGMPLdQULCQgHAgIi
AgYVCgkICwIEFgIDAQIeBwIXgAAKCRCzCjXGIZinfDHSD/4u7/jIRUrSQDm8vvex
CREIvq0p+ND/OStk1vVdDOYe9lao3ZZvuogtM+gaFh71E1bLOPBym5WPgASjs/LD
xqbKcFoWWW5+Wi6KNg/NGuT2PAL3dRunN3dJSB6kVC6CUiMiZjuuHtItac2qOn7z
Q2mClf+L8zKhfMTbHC0fpOZ0aBJZpHBGVQqjF+HLKQWiFTJPHtSFWOepkqyFAhtT
wRcBdD6/f27luv8kC6WMD4fzCMR2gBwqAvAboWadq2tG991cfwa5Sd3NAkZI61mQ
mSy2J5lagleYVMEaY/j/OaD8Z78N01AIVKz0mAEnwR2h1LyYwl6g6yRw6ya6wbFP
RCJcc1kXF9nJg9f9//8aSt3ZsMZtUWJrBwO10dpaJqGE3Wez148gLS2S7qvFwZ1g
ShjUkIr+2e7zUurO423jkHls/y5pBDLD1gbATBaAq6H/oELwFx3Ypzb5pk+g+afd
sVEu2quix4QgM5iiLT3ZaiLAviUL+M2cqDjYHbCaa2k1HfMWtLFBv9xVwDE/alAd
ZjS0lUV+By2h1kKrgzA3+JUsZEzb8oqagNz6ury8gc43uzmTIKizdnMVpX6EWWiL
dkYr0hJf1AtDRFJAf6DlQqrGElAZgX0PZQwZFTrb2Dla3oucDnkvjpCF2OJCzFKj
676QKPN54Lr42C3j148Ttr5qUrkCDQRjV59bARAA1JuAkQUdpSAmNPh4DGX5Kkvy
drvA9Nc9q+RHkSMUiHTsBdw1F4mb22Pz9rjwmwPUOksnyEGDAmPOilvuT5vihPX+
oKC6/RFMRixEQ32K799xV+SqQd2W1VfZyfZdIGNawDwIHXkd/9komJgCW3xCZPWX
zsvgJxqV0EYUIoa8uzYKUmgsNa1a2jcCCoqojPdW3zWhjPmtVlfFqLq87dksofP9
JYWbvEKms8F7fbKCrB4mUgjySiXX7n/CLSHNRWF34zwg1E/aq1a/jBkKYROjBN/Q
nvkfeA0jywPtd7bo2cIbYstvJEL32JgB33/rkaXT9/IbB03T+pCs1VfAfx9XL2ro
ZywsxqoRiwTiJnPeYTKGRptWj7aA5A7SCs4WLN+f9KBeevk6jm3xgSxpfEqFkGlk
xSh1rQX0OShwgHs0ylsOAXD+PTbynoEMTkVmb3LClvKQ/e8hnIcEs32YnyaO8c/J

id1Nsf6ECCTwZ6OLgiVLYFPJ2yB6/wCxV7rdTpsjK8zSmSr3V66BpEiXB+W3k8QV
Z9WWpRg2Nl9r8HgV8UICeUq4Unbr996JaYSdXMmF1PRDJSh69uDxwodkNAF3jWyZ
ysdZsMPSwLYhpxareuAIr7ktpjj77PEhxZ2sVupsgY0u3cKeoJm8KFes8o3v/1db
8R4g9wWPf1dBsWb0yOkAEQEAAYkCPAQYAQgAJhYhBB0PFHINeAL/wG238rMKNcYh
mKd8BQJjV59bAhsMBQkYw8t1AAoJELMKNcYhmKd8PscP/0HMwFExqgU1F6kYXWVT
qUrH1qTcD1uY9vbI9Gew1dK1P8/eUlMEpgePfGsIlzyFs9lMcjVDgJ5/tDOO/ayC
OIi2FXgPIyegAaktyy+AeKhPp8kglF6Wxv1H0wNPo87h7DSJPjp8Z5LDkwRlG+pF
SsA9aqKlkzyY6r67BQIcAbHBpzY6neqnN5p8WPuEcB+mCqet2EH5fvRVoIPiArhU
/UZ0uUZUyw9eBoP27NKm6mbyA35ThJLwedhb3cq9qOwR7ARIOGXS4qyk/VzCqvSM
VM9pJlJsFFDrxtfH5TMUzf0Rq8huYSYt/oMcRtR437bG5mv1fWEQuWpwM0Q26Zhy
d/Ur2aCFprD1B4KKi6+3cg2OGAvnsOOFXQiPfUNulg//s+dMdzaCvMgvf9xh17VT
Kt0tmA808H9VCfnU6cDLvjX/ybNVs0JnuIHZMVwWo3wGu7BTBGVKi2PG9XOGInwA
xE1O45O9buJ8kbn+z9ORxLmgfBBMv+TNBx3C40gMPTNMkSNa1MpLHHI8V03PBs3R
tyo5TxQAcDu2e+Xnr2GpM2FKgqS7Utuyc3JDS7Qvz+mTPg3IVllLjii7rQNy2r6Z
iSopndXdiI3CCz9d9HzseQaEM0hRm0c7pEEN2XlkwZOehnHcYuA1Y/Ohdu+4Hnjc
/NOI/QVZGETbgNuq+Wygim+t
=cneg
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.perhutani.co.id/publickey.asc

2.9. Anggota Tim

Ketua Perhutani-CSIRT adalah Direktur SDM, Umum, dan IT. Yang termasuk anggota tim adalah seluruh anggota Perhutani-CSIRT.

2.10. Informasi/Data lain

(Tidak Ada)

2.11. Catatan-catatan pada Kontak Perhutani-CSIRT

Metode yang disarankan untuk menghubungi Perhutani-CSIRT adalah melalui *e-mail* pada alamat csirt@perhutani.co.id atau pelaporan melalui aplikasi Help Desk TI Perum Perhutani pada alamat https://layanan.perhutani.co.id.

3. Mengenai Perhutani-CSIRT

3.1. Visi

Visi Perhutani-CSIRT adalah terwujudnya pengelolaan keamanan informasi yang andal dan efektif di Perum Perhutani sesuai dengan prinsip keamanan informasi.

3.2. Misi

Misi dari Perhutani-CSIRT, yaitu :

a. Mengkoordinasikan penerapan insiden keamanan siber di lingkungan Perum Perhutani
b. Membangun kesadaran keamanan informasi pada sumber daya manusia di lingkungan Perum Perhutani
c. Menjadi pusat pelaporan serta penanganan insiden keamanan informasi di lingkungan Perum Perhutani

3.3. Konstituen

Konstituen Perhutani-CSIRT adalah pengguna layanan TIK di Perum Perhutani.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan Perhutani-CSIRT bersumber dari Anggaran Perusahaan.

3.5. Otoritas

Perhutani-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber di lingkungan Perum Perhutani.
Perum Perhutani-CSIRT melakukan penanggulangan dan pemulihan atas permintaan dari konstituennya dan dapat berkoordinasi serta bekerja sama dengan BSSN / *Principal IT Security* / Ahli *IT Security* untuk insiden yang tidak dapat ditangani.

4. Kebijakan – Kebijakan

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

Perhutani-CSIRT melayani penanganan insiden siber dengan jenis berikut :

a. *Web Defacement*
b. *Malware*
c. *SQL Injection*
d. *Phising*
e. *Spamming*
f. *Network Incident*

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

- Perhutani-CSIRT akan melakukan kerja sama dan berbagi informasi dengan Gov-CSIRT atau CSIRT lainnya atau organisasi lainnya dalam lingkup keamanan siber;
- Seluruh informasi yang diterima oleh Perhutani-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

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

5. Layanan

5.1. Layanan Utama

Layanan utama dari Perhutani-CSIRT yaitu :

5.1.1. Layanan pemberian peringatan terkait dengan laporan insiden siber

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

5.1.2. Layanan penanggulangan dan pemulihan sistem

Layanan ini diberikan oleh Perhutani-CSIRT berupa koordinasi, analisis, rekomendasi teknis, dan bantuan dalam rangka penanggulangan dan pemulihan sistem.

5.1.3. Layanan penanganan kerawanan

Layanan ini diberikan oleh Perhutani-CSIRT 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 penanganan kerawanannya tidak dapat ditangani.
b. Layanan penanganan kerawanan yang dimaksud dapat juga merupakan tindak lanjut atas kegiatan *Vulnerability Assessment*.

5.1.4. Layanan penanganan artifak

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

5.2. Layanan Proaktif

Layanan tambahan dari Perhutani-CSIRT yaitu :

5.2.1. Layanan *Security Assessment*

Layanan ini diberikan oleh Perhutani-CSIRT berupa identifikasi kerentanan dan penilaian risiko atas kerentanan yang ditemukan.

5.2.2. Layanan *Security Audit*

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

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan oleh Perhutani-CSIRT berupa pemberitahuan terkait dengan ancaman baru insiden yang ditemukan melalui hasil monitoring dari sistem deteksi dini keamanan.

5.2.4. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini diberikan oleh Perhutani-CSIRT berupa penyelenggaraan workshop keamanan siber dan sosialisasi keamanan siber kepada konstituen.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke email csirt@perhutani.co.id atau dengan melaporkan ke aplikasi Help Desk TI Perum Perhutani pada alamat https://layanan.perhutani.co.id dengan melampirkan sekurang-kurangnya bukti insiden berupa foto atau tangkapan layar atau log file yang ditemukan.

7. *Disclaimer*

Disclaimer terkait penanganan insiden siber tergantung dari ketersediaan *tools* yang dimiliki oleh Perum Perhutani.