RFC 2350

Cyber Security Incident Response Team Yayasan Pendidikan Telkom

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi *Cyber Security Incident Response Team* Yayasan Pendidikan Telkom berdasarkan RFC 2350, yaitu informasi dasar mengenai *Cyber Security Incident Response Team* Yayasan Pendidikan Telkom, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi *Cyber Security Incident Response Team* Yayasan Pendidikan Telkom.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 3 Oktober 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk informasi pemberitahuan RFC 2350.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.ypt.or.id/rfc-2350/ (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik *Cyber Security Incident Response Team* Yayasan Pendidikan Telkom. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 *Cyber Security Incident Response Team* Yayasan Pendidikan Telkom;
Versi : 1.0;
Tanggal Publikasi : 3 Oktober 2024;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Cyber Security Incident Response Team Yayasan Pendidikan Telkom
Disingkat : Komite CSIRT YPT.

2.2. Alamat

Jl. Cisanggarung No.2, Citarum, Kec. Bandung Wetan, Kota Bandung, Jawa Barat

2.3. Zona Waktu

Bandung (GMT+07:00)

2.4. Nomor Telepon

(+62) 822-4002-1192

2.5. Nomor Fax

Tidak ada

2.6. Telekomunikasi Lain

Tidak ada

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

csirt@ypt.or.id

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

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Encryptomatic OpenPGP Add-in for MS Outlook 2.7.17.0

mQINBGcPb9cBEACYfLsl87ku7yqrGei427AvrhSVzEAoxlyF8rO5S8hRdUjL613d
iMa2VJ4I8mS7ybY+zGaafarFDz4Ti6f8slh199rgnkwArStVG4onUjg2obJMlZe5
RPmjYb2RrJZsQKT6C4z7f6ix6b8d1ZJ3fjLB9QLVnm8P5YQ+nZxlEQQ495u0wkC+
a3E7cy+qvUS+WQuyhSGbp9P+oKGqewSkEwhzIwZn4rtXS1EAsBko65K9eyFqH8
aZ
bHgeTEzN/4yOgcuM722Om9lsvjNQ33Rbfcm4aI5LZHzFJdYZAZVmzLFvyO2wXkC
r
76K3uVhg51ZNedMbQLHu3LIFS13PT9YF5IurXu80cw5IsAGBdFlmOu1wiwiSNbE8
lD7ZvrZDi/lKBNMKayMQR+IuVe82CiC7vtquC2uyYGjgJUlfIVjZBc2+G7bpQTY2
bxe6hrsaZpypsee7dFwGYrlDTgH1snmp84sLfs63/NU3z50hgFAj6bBVCHcXGPat
MRTJeMNMUJorGWcsvoFJu3XzKS1vfD1lwMBmUdUH70Hv475qBALi55xwm637
MLYH
dieKAcAc6fuz948SInJ1WSmK+9i6jhzZ7s67zUM0l1Mn5FgilM9cXwRzXoPz0In+
FITvDPIOKv5+9xXPHV245Vck8uYhmp7Z1kv9ELWt33OLCmsasXZOQwbu5QARA
QAB
tA9jc2lydEB5cHQub3IuaWSJAiIEEwEKAAwFAmcPb9cCmQECGwMACgkQxvOPG
2pU
vtFcOg//QBecyuwViajOW2v7b7qDTIbZhUWnQPnsqzn8Bo7zvf1veByJq5iewR/P
AEUOPBZEABk1GQfDiZfliYL1v7Pr445KYBDKRHxEqq/v+WTTFXsHz+B7JcU8Fu1
L
+l4mUYSCeD6s4T6X3jDCnxd9DVb71vOp5jsSfHJsKvGcz0qUokNjG7brRM2YwbK
6
i1juYh3qOHhW+xsacW6TbBvhV2wWEgpyy9ytoeq4scK/roFYNOiL1IRgO55YsxwT
O+FiaOb27fKK4BG8ndlg5FCd9dmwUQ+Dqt7O/cUEPor7YLZ94fXMoBsOHIf1CrRv
eYDlo8wI6YWmrNUSJwMjOfyKI4X4SZyIU65CnNWuXXCalrlyP5bsLJ7vUz6xq2GA
wX2t7py4RneUyeYMPV+k5fuLNRBtLvHuXCx7iiKE8NFr9O/Wag9zOzimzn5ViTRk
bjcTXxVsBSK3bm9sbgDEE0mmGPuWzbweiCxYFIiugT539BPK6Ahvo7U8EoOkw7
xc

i1IJyyWJUVeh5dZmHgTXy8GzjUQw/oZcVPGfyW3G+/1V01ZwJha6qTi7X8UMrAW
T
6zHHPIIltr8m+c/rWc3U+MyWiD/ghYumWBJqwT8J9QfKaYgEoq1RhP4tKjmH8Gty
GOEAKazhHV4l6rAXkqMFW49+l3RccjEr3oHdyWNECmr3Nz52Osm5AQ0EZw9v1
wEl
ANQddkMT82/+z3VRXlHlkmAqeNynJFRschSMNUApvJxwCBbQlirACzoCr2rH+7d/
VByVfAb6w+WDsnmUqV8LbjRpk/BHVJ0ggKakpSGOzAmFdHA8DRk3TldYa6ywJ
YZJ
2i7QdI0efRr31HcRrzBwMM30+rNqxTYDlBkQl8fJBKrfUJnklfHSyeDaE7TKvGDl
dgmzP6CcjEk9WXnFyyvb9rWTJvVNkofhbswia4gDWALIhE2m7aoQB8AKij4uKKOo
xaPObiVgJnMa3BTmhp6siffhEKB0YdjpUg/kBRqL3MDrXN/5vlKEhkeUJaU5jU1X
8qWoSG3L6nZO3M7hTCKL+bsAEQEAAYkCHwQYAQoACQUCZw9v1wIbDAAKC
RDG848b
alS+0c+nD/0fiAZTHPrn4oFCuhIJAx0WEY7T0tR9lPuty3y/m2vnO4lIWUkqVtdf
6c9Cff7KiUMZdOSe1ADwdNdHIfXOVQEzZUeWkAsuxMwx6PoHPBjJPHORz+1v3v
WT
U/6Xp4UG9IA+8Jn2MR1001CWrw3bemY36Cp00J6OS6hjzypQFkmKB86yZg/mCff
+
KyKp2Cc/lRZ2+0XD8jz0TLmlZOqNl8JUeDEFF4VmC2A+AYrwGguhB15KdAHHRO
1B
eCfpZfSxAkKW0n7d5VsqedJ3DIwfeEM8HhH3gF+TIaPmjoKjIUdcbaXULpDUgyTq
/4fvtFYuQ0jRadyQ3hGjsnAdX8IfV8yl7c0qx+equfbcuk1KbVmHL+Wpu1Q92eJ2
w3RZvjDddHO1q02lYRmxaNVBTaJBgGuVkyWcwFLJjuwLGvZd+Ncqso5MVBP6w
w6p
9vGskjFtmze9QAE4indldIVZMJGB+KZsweGo3RV7Bd+ls/H7JcdoNqWuxjEydvDy
RJLaHwyFkOh5rGjfwB1FihuQ5+AlAPej+txvkEsf+1tA/t7AlDAw7nn8frSbT3uV
pvxsWPan+tFe3UJQdWZHsHUA8sn3y6bqW1xDhNNl2RrkxSICpGI6Yi8WfhTyeD0
4
QUGm7qcAC+OtetHHe6VSYqyvbwO6WrGmZYjxcAuncRpSy+tLOh48Lw==
=gfc8
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.ypt.or.id/pgp-public-key/

2.9. Anggota Tim

Pengarah	:	Direktur Utama YPT Direktur Shared Service YPT Direktur Strategy and Education YPT Rektor Telkom University
Ketua	:	VP Information Technology BPK
Wakil Ketua	:	Direktur Pusat TI Tel-U
Sekretaris	:	AVP IT & Security Strategy BPK
Koordinator CSIRT BPK & TS	:	AVP IT Infrastructure BPK
Koordinator CSIRT TC	:	Kabag Infrastruktur TI Tel-U

2.10. Informasi/Data lain

Tidak ada

2.11. **Catatan-catatan pada Kontak** Komite CSIRT YPT

Metode yang disarankan untuk menghubungi Komite CSIRT YPT adalah melalui *e-mail* pada alamat csirt@ypt.or.id atau melalui nomor telepon ke (+62) 822-4002-1192 pada hari kerja jam 08.00 - 16.30.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi Komite CSIRT YPT adalah menunjang dan meningkatkan kualitas lembaga pendidikan di bawah naungan Yayasan Pendidikan Telkom.

3.2. Misi

Misi dari Komite CSIRT YPT , yaitu :

a. Melakukan koordinasi dan supervisi dalam penyusunan strategi pengelolaan Information Technology seluruh Lembaga di bawah naungan Yayasan untuk mengembangkan teknologi informasi.
b. Menyediakan sarana dan prasarana yang diperlukan untuk mennunjang proses pembelajaran termasuk penggunaan teknologi informasi dan komunikasi.

3.3. Konstituen

Konstituen Komite CSIRT YPT meliputi Badan Pelaksana Kerja dan seluruh Lembaga Pendidikan Dasar Menengah (Lemdikdasmen) di bawah naungan Yayasan Pendidikan Telkom.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan Komite CSIRT YPT bersumber dari anggaran unit IT Yayasan Pendidikan Telkom.

3.5. Otoritas

Otoritas yang dimiliki Komite CSIRT YPT meliputi:

a. Penetapan keputusan mengenai perencanaan dan implementasi program *Cyber Security Incident Response* di Lingkungan Yayasan Pendidikan Telkom.
b. Koordinasi seluruh kegiatan perumusan dan penyusunan Program *Cyber Security Incident Response* di Lingkungan Yayasan Pendidikan Telkom dan melaporkan hasil pelaksanaannya kepada Pengarah.
c. Memastikan kecukupan kebutuhan sumber daya untuk implementasi program *Cyber Security Incident Response*.
d. Koordinasi dengan pihak internal dan eksternal yang terkait dengan Program *Cyber Security Incident Response* di Lingkungan Yayasan Pendidikan Telkom.

4. Kebijakan – Kebijakan

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

Komite CSIRT YPT melayani penanganan insiden siber dengan jenis berikut :

a. *Web Defacement;*
b. *Distributed Denial of Service* (DDOS);
c. *Malware;*
d. SQL *Injection*;
e. *Data Breach*;
f. *Phishing*.

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Komite CSIRT YPT akan melakukan kerja sama dan berbagi informasi dengan CSIRT dari kementerian dan atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh Komite CSIRT YPT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa Komite CSIRT YPT dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon. Sedangkan untuk komunikasi yang memuat atau mengandung informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail (sesuai subbab 2.8).

5. Layanan

5.1. Layanan Utama

Layanan utama dari Komite CSIRT YPT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh Komite CSIRT YPT untuk memberikan informasi dan peringatan akan adanya insiden siber kepada pemilik atau pengguna sistem elektronik dan informasi statistik yang dikelola oleh konstituen.

5.1.2. Penanganan Insiden Siber

Layanan ini diberikan oleh Komite CSIRT YPT berupa koordinasi, analisis, dan rekomendasi teknis dan bantuan *on-site* dalam rangka penanggulangan dan pemulihan insiden siber.

5.2. Layanan Tambahan

Layanan tambahan dari Komite CSIRT YPT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini diberikan oleh Komite CSIRT YPT berupa koordinasi, analisis, dan rekomendasi teknis dalam rangka penguatan keamanan (hardening).
Layanan ini hanya berlaku apabila memenuhi syarat-syarat berikut:

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.

5.2.2. Penanganan Artefak Digital

Layanan ini diberikan oleh Komite CSIRT YPT berupa penanganan artefak digital dalam rangak pemulihan sistem elektronik terdampak atau dukungan investigasi atas insiden siber

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan oleh Komite CSIRT YPT berupa informasi statistik hasil deteksi dini sistem monitoring kemanan siber atau informasi dari tim CSIRT kementrian atau organisasi lain yang perlu diwaspadai oleh para pengguna sistem elektronik.

5.2.4. Pendeteksian Serangan

Layanan ini diberikan oleh Komite CSIRT YPT berupa informasi statistik hasil pendeteksian dan monitoring keamanan siber.

5.2.5. Analisis Risiko Keamanan Siber

Layanan ini diberikan oleh Komite CSIRT YPT berupa laporan hasil analisis dan identifikasi kerentanan dan penilaian resiko atas kerentanan yang ditemukan.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan ini diberikan oleh Komite CSIRT YPT berupa pemberian rekomendasi teknis berdasarkan hasil analisis atas resiko kerentanan yang ditemukan terkait penanggulangan dan pemulihan akibat insiden kemanan digital.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini diberikan oleh Komite CSIRT YPT berupa informasi dan publikasi berbagai kegiatan yang dilakukan dalam rangka membangun kesaduran dan kepedulian terhadap keamanan siber.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke csirt@ypt.or.id dengan melampirkan sekurang-kurangnya :

a. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan;
b. Atau sesuai dengan ketentuan lain yang berlaku.

7. *Disclaimer*

Penanganan insiden dapat dilakukan berdasarkan ketersediaan *tools* yang dimiliki.