RFC 2350 YakesTelkom-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 0.0 yang diterbitkan pada tanggal 18 Juni 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://csirt.yakestelkom.or.id/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditanda tangani dengan PGP *Key* milik YakesTelkom-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 YakesTelkom-CSIRT;
Versi	: 1.0;
Tanggal Publikasi	: 18 Juni 2025;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Kepanjangan dari Yayasan Kesehatan Pegawai Telkom-CSIRT
Disingkat : YakesTelkom-CSIRT.

2.2. Alamat

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

2.3. Zona Waktu

Bandung (GMT+07:00)

2.4. Nomor Telepon

0821-1566-7778 / 08135-4881-849

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

WA/Telegram (0821-1566-7778 / 08135-4881-849)

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

yakestelkom-csirt@yakestelkom.or.id

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

Bits : 2048
ID : 0xBE19B537D16D1EB4
Key Fingerprint : 829D F882 01DA 9275 807F DB6B BE19 B537 D16D 1EB4

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

xsDNBGhI35kBDACy5mFI5Iku8Ynk7JrRuoD7ytvSfsJ3a9JgOSLKSn0ILzAxmEZq
D9qp747HOwaIho4Nxv1yyOTpXd0vVl48RBnlQ4s4dLo/JNwARLTJ4+jSkMmlnzHN
3Ng6VMDTOvpHo1oebMUJ776G65KAH6ySFWYvL10Lj+BI9MAYM5bzlPCOET7fxc0r
+UDg75fLOqs5VbZCjzHstVaWl4bxyQ2drwu30Hy5OozxlXcFqDrOltbEkcF3jijZ
12Lawe37aIUOm3tban4YvmNL/8+U/YFpUR/+kMsoperqm4ReuUOep6Bx40j1eLD7
UisyHm9T5G/lihDG/LzvbbZE7LQ8kZs5IRq4fJpzZF2fwpALkNsgRLyROBQF9gVY
/+HGFKZUMmzYgNrBsLYkHRQHu+ZZGzr0TWq4duiMBeqQJtSM9/quQ9uXHJH5Wq5J
kDn5BxsgYbG20GBI5sw2E57WpGYVetvrE3NiHl/ylgzTyI7aUQRU/9XEDcIZlPQ8
pQ8c+7cpGf5yvCkAEQEAAc03eWFrZXN0ZWxrb20gQ1NJUlQgPHlha2VzdGVsa29t
LWNzaXJ0QHlha2VzdGVsa29tLm9yLmlkPsLBDQQTAQgANxYhBIKd+IIB2pJ1gH/b
a74ZtTfRbR60BQJoSN+aBQkB4TOAAhsDBAsJCAcFFQgJCgsFFgIDAQAACgkQvhm1
N9FtHrQqbgv/cC0kdOgscJPlKgZzspAeyuixpd8R93WcL1AkQDoqJ88ywJmWNgcd
Ah/2iPdLCAI3jybNh9Jf529rXEu4sTRK2q0AJH5Uwm66WN+Me8ba1D5f2ZZeDIFE
aeSgMRoSkiyoqTuUrW+agQIR7WLuuHo04IANDsd2sXHWFJ57agGzUQHzAGDBuOmN
aEkaLj4n5fKZ7YcPbvpv6p8lYKQ3isDPKht6oK8tym6sEC4ammBiydrqShrlBxpX
RjVosl08bEh8X8vvcaYL8wdSoaetcwTdslbHJWBS4ZaZlP7F+fozaWf8dswGb1xJ
4rgUOfd5SYXxgY3v4dHrBoZRilj3HQNHr1Fw2CMdG0IJ7flMUjoZgb6M4He+V88R
yu/RMD5pdfTmmtW3H3A/xz0QMCT+5xkhsCr2q0U7jo7XscsTcGg2rhJcYf9tIs8H
LK1fO+kcqewqbRCBmztD7+qBpdpWRDu48rkKWVl7IotUTeiGgEG9xV4AJA/ghAXt
A4caXetkH9LfzsDNBGhI35oBDADuu+FfVKFxDZiiVIPmLH6+GHJ6KJ/krwVJDjgQ
LII8OiITL4YC51FrX32kQGJQNWIdr8fZAG0MWIoPGmEpb2lzKMZzFXExqAwoMNb7
nbOJvuAWQnkAJFUc5P+zXnUBcdynMS9zIq71Qqd91rlCrdCSP3nEcYgBRP/syndf
yuTCX151Ibz39PzALME7LCzCq6QPoPvKi7V4+0ErxYsKLTQ4/q0T5fb1b0eOm034
a+B/V3UNEAT6AQ2ua7gvNTgcRm8ruWil/t0uX0kutFAspp0CrfQvureLYJrNQWhT
OV2dj8z+9qamTtINM45XL52DkBg4Hj5sCqDHk/9ku2P6SzED9Orq/Jee9X+qLNdK
qfIbspDgm31VatEKV8K5/qldKhyyxorUrQ8J+tCjIAOeiP/qdXij4r2/7wskOEBE
eXujFue33DcLhj1LbyADLtxuOCGCBba/88yHySaxWF/D90Z+WmHCgMPpErvxa0C4
HumSYJ9AV8qlQmP55WhuLgknhXcAEQEAAcLA/AQYAQgAJhYhBIKd+IIB2pJ1gH/b
a74ZtTfRbR60BQJoSN+bBQkB4TOAAhsMAAoJEL4ZtTfRbR60booL/i6UlWnzXkbe
l4jDCInqgVexkwIhc4i8CIr1/+DadUbmQQ/f9wCM6oInpj7IOyCCgSiz7WUSr3V+
/ajUWvWKRkPrm7A7z8M3YZa0bvbpC2i0tZ/5KBlH1A6CaNEP5SMcSfXBUhzfmAuw
GP9mNPt8VwoQA31Vz3FyPF5n1ThRdikjc4u8SiE0/8USJzAgS5LRYzW5pz/7yJIs
f5HzzJifeTLc0DIed+ufivifwlNyS++MpfZWzBaxGorFtp1OTIGHoowDcb4dUV3I
QlM3QeG4d9igNISBX8nPmBMVGVQEGkpYY7GIWKWvXjbuwHvMeHCj6ZDIbZJDv1oN
32bp7+5eZvjdHvMTx792aUixC29is3/y6Fwakc0qpJ9p9jJSf5pzCcXk2xXbHdaK
EY6L8EwCi9hjBfQ7iNZnFa+PtJ1bT63cgHIx8itOAFQqxdDi551ed+4FWvQHzp0J
bfSeS35S1LoUg+QQbm9olC96SmML7NigjS2gFNaDYA1xCz0XD1OjEQ==
=ujR9
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://csirt.yakestelkom.or.id

2.9. Anggota Tim

Ketua YakesTelkom-CSIRT : OVP Customer Engagement & Digital Experience. Untuk anggota tim merujuk kepada Surat Keputusan Direksi Yayasan Kesehatan Pegawai Telkom Nomor SK 08/PS000/YAKES-00/2025 Tentang Computer Security Incident Response Team Yayasan Kesehatan Pegawai Telkom (YakesTelkom-CSIRT)

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak YakesTelkom-CSIRT

Metode yang disarankan untuk menghubungi YakesTelkom-CSIRT adalah melalui *e-mail* pada alamat yakestelkom-csirt@yakestelkom.or.id atau melalui nomor telepon 082115667778 ke Helpdesk IT pada hari kerja jam 08.00 - 17.00 atau emergency 081354881849 ke Islahuddin siaga selama 24/7.

3. Mengenai YakesTelkom-CSIRT

3.1. Visi

Visi YakesTelkom-CSIRT adalah menjadi tim tanggap insiden siber yang terpercaya, responsif, dan proaktif dalam melindungi infrastruktur dan informasi organisasi dari segala bentuk ancaman keamanan digital.

3.2. Misi

Misi dari YakesTelkom-CSIRT, yaitu :

a. Melindungi aset informasi dan infrastruktur TI Yakes Telkom dari potensi ancaman dan serangan siber.
b. Meningkatkan kesadaran dan kapasitas SDM di lingkungan Yakes Telkom terhadap keamanan informasi melalui edukasi dan pelatihan.

3.3. Konstituen

Seluruh unit kerja, sistem informasi, dan infrastruktur teknologi informasi yang berada di bawah pengelolaan YAKES Telkom

3.4. Sponsorship dan/atau Afiliasi

Pendanaan YakesTelkom-CSIRT bersumber dari anggaran Operasional Yakes Telkom

3.5. Otoritas

- Menetapkan arahan strategis program keamanan siber Yayasan;
- Menetapkan strategi, kebijakan, dan prosedur penanganan insiden keamanan siber;
- Memberikan keputusan strategis selama terjadinya insiden;
- Membangun komunikasi dengan pihak luar seperti CSIRT nasional, lembaga regulator, atau Mitra jika dibutuhkan;

4. Kebijakan – Kebijakan

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

YakesTelkom-CSIRT YAKES Telkom menangani berbagai jenis insiden keamanan siber, termasuk namun tidak terbatas pada:

- Malware dan ransomware
- Phishing dan spear phishing
- Kebocoran data (data breach)
- Serangan DDoS/DoS
- Eksploitasi kerentanan perangkat lunak
- Akses tidak sah atau peretasan
- Penyalahgunaan hak akses internal

Dukungan yang diberikan oleh YakesTelkom-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden. Tingkat dukungan yang diberikan tergantung pada tingkat keparahan insiden:

Level	Deskripsi	Tindakan dukungan
Kritis	Menganggu layanan utama, berdampak besar pada layanan Kesehatan atau data sensitive.	Respons segera (<= 1 jam), ekskalasi ke manajemen, koordinasi lintas tim.
Tinggi	Berdampak pada beberapa sistem penting, belum menyebabkan kerusakan data.	Penanganan cepat (≤ 4 jam), investigasi menyeluruh
Sedang	Gangguan terbatas, berdampak pada sebagian pengguna.	Tindak lanjut dalam waktu ≤ 1 hari kerja.
Rendah	Tidak berdampak signifikan, namun tetap perlu ditangani.	Monitoring, dokumentasi, dan analisis berkala.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

a. **Cooperation and Interaction:** Terbuka untuk kolaborasi dengan CSIRT lain, instansi pemerintah (BSSN), vendor keamanan, dan mitra terpercaya sesuai prinsip kerahasiaan dan kepatuhan hukum.
b. **Disclosure of Information:** Informasi insiden hanya akan diungkapkan kepada pihak yang berwenang berdasarkan prinsip need-to-know dan kebijakan internal organisasi.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi bersifat biasa dapat menggunakan email yakestelkom-csirt@yakestelkom.or.id atau WA 0813-5488-1849. Namun untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakann enkripsi PGP pada email.

- Identitas pelapor dijaga kerahasiaannya jika diminta.

- Pelaporan ke pihak luar (BSSN, Kemenkes, dll) dilakukan oleh pimpinan CSIRT setelah verifikasi dampak dan eskalasi.
- Setiap insiden harus didokumentasikan dengan **bukti digital (log, email, tangkapan layar, dsb.)** dalam 5 hari kerja setelah insiden selesai ditangani.

5. Layanan

5.1. Layanan Utama

Layanan utama dari YakesTelkom-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Memberikan notifikasi kepada stakeholder tentang ancaman atau kerentanan terbaru (zero-day, malware baru, dll), menyampaikan buletin keamanan regular dan mendistribusikan informasi dari BSSN atau mitra lain.

5.1.2. Penanganan Insiden Siber

Menangani insiden keamanan siber secara cepat, tepat, dan terkoordinasi untuk meminimalisir dampak**,** memulihkan layanan**,** serta mengurangi kemungkinan insiden berulang. Tahapan penanganan insiden diawali dari identifikasi, klasifikasi, eskalasi, penanggulangan/isolasi, pemulihan, pelaporan & dokumentasi dan evaluasi & pencegahan berulang.

5.1.3. Penerimaan Aduan Insiden Siber

Penerimaan pengaduan insiden siber dengan penyediaan formulir pelaporan insiden secara daring dan email pelaporan khusus, melakukan verifikasi awal terhadap validitas dan urgensi laporan, membuat tiket dan tindak lanjut awal berdasarkan tingkat insiden serta koordinasi dengan pelapor hingga tahap penutupan insiden.

5.2. Layanan Tambahan

Layanan tambahan dari YakesTelkom-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Melakukan assessment berkala VA melalui tool VA, laporan pengguna dan notifikasi mitra, Telkom atau BSSN.

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

- Memberikan informasi dini kepada seluruh pemangku kepentingan tentang adanya **potensi ancaman siber** yang dapat memengaruhi sistem elektronik organisasi.
- Pemberitahuan ini bertujuan agar langkah mitigasi dapat dilakukan secepat mungkin sebelum ancaman berubah menjadi insiden nyata.

5.2.3. Pendeteksian Serangan

Mendeteksi secara dini aktivitas atau kejadian yang mencurigakan atau berbahaya yang berpotensi merupakan bagian dari serangan siber terhadap sistem elektronik organisasi. Pendeteksian dilakukan melalui pemantauan log & system, system deteksi serangan, dan threat intelligence.

5.2.4. Analisis Risiko Keamanan Siber

Menilai potensi ancaman terhadap sistem informasi organisasi dan menentukan seberapa besar dampaknya terhadap keberlangsungan layanan, agar pengambilan keputusan keamanan dapat dilakukan secara **berbasis risiko**.

5.2.5. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Melakukan Pelatihan kesadaran keamanan kepada seluruh karyawan, melakukan simulasi tanggap insiden (tabletop exercise, red teaming) dan panduan SOP keamanan dasar (misalnya pengelolaan kata sandi, penggunaan email aman, dll).

6. Pelaporan Insiden

Laporan insiden dikirim melalui kanal resmi (formulir online/email ke yakestelkom-csirt@yakestelkom.or.id atau WA 082115667778).

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan

7. *Disclaimer*

Dokumen ini disusun oleh **YakesTelkom-CSIRT** sebagai bagian dari komitmen terhadap transparansi dan kesiapsiagaan dalam keamanan siber, serta untuk mematuhi formatstandar RFC 2350.

Informasi yang tercantum di dalam dokumen ini bersifat informatif dan tidak mengikat secara hukum. Konten dapat berubah sewaktu-waktu mengikuti perkembangan kebijakan, struktur organisasi, atau kebutuhan operasional **YakesTelkom-CSIRT** .