RFC 2350 VNCOOL-CSIRT

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 31 Desember 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

Untuk internal organisasi perusahaan serta pihak-pihak terkait yang berwenang, termasuk ICT CSIRT dan Nat-CSIRT, dalam rangka koordinasi, pertukaran informasi, dan penyampaian pemberitahuan terkait keamanan siber.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :

vncoolid.com

1.4. Keaslian Dokumen

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

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul : RFC 2350 VNCOOL-CSIRT;

Versi : 1.0;

Tanggal Publikasi : 31 Desember 2025;

Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Kepanjangan dari VNCOOL- Computer Security Incident Response Team

Disingkat : VNCOOL - CSIRT

2.2. Alamat

Jl. Cideng Barat No.114, RT.12/RW.1, Cideng, Kecamatan Gambir, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10150

2.3. Zona Waktu

Jakarta, GMT+7

2.4. Nomor Telepon

+62 821 4567 5280

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

-

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

vncool-csirt@vncoolid.com

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

Bits : RSA 4096 Bits

ID : 0x68A4000E9958157A

Key Fingerprint : 363D 7DB4 EC13 DDB2 9A0F 450F 68A4 000E 9958 157A

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

xsFNBGloZCMBEACqo8FCQhlpMsjTRyrxl4ZUTCrwVbCP+ufMZp/3HMmCsqRlaGx0
dhlwa/bE0FUWKqEgAGHE3gaIF2RuYu4ZiWg8CDcn2qmQsj7U9RCJmq9niQg3c+Pn
v48uPT5WyxPbRtCml8DeH+98SWP+1HB6lKX3Cx4rOI7SKjSbQZzSVgOYm+52Mu8c
9w4g5nq/ycOuqhhNgq3u2jHXIPa7+E3aSSA3OmwGQAr2kVSm24k7HvKpY6rvcYyG
gsHCgOTzP8fah2wmhk3JSZgzVQClOxHXSGJ50RsTh3FXGdR4m7tNZ2d/BU9rF42K
a3gYyln6u+Rtc22O3z1mVHhSR3ssqWo6gBWZEGWmmt80EBIRGSEnHiFh28HeyNjy
BN1G8gTHDEP8u4cwQPEgHdtYtU8/243ZXxrCeoISbrhLPJbvBjyjBckRHSuxoBCb

+rZ7xwCX6pfgGkD+WFAcFawOeeyFFj03GU+RZjMTcIGaCftesRe4CH8dKqSkkd85
COTKtPlTJXaGz3WNz4pzfg+MnTGEiGkCNLVbMhw9BsqTrWSl1Vlb3P5FrvjMhbos+lLnQdpWs+jw4rh/suBg+EaHCkIaHrcSvTpGbSLjac5Cd1oFYAVBQePc8k1UeW5svSuJniuvQDE+ftMp1aw4MxuYBbN1staZtSjIyPZHPTd0ilDlmnwRk/YY1QARAQABzSh2bmNvb2wtY3NpcnQgPHZuY29vbC1jc2lydEB2bmNvb2xpZC5jb20+wsGNBBMBCAA3FiEENj19tOwT3bKaD0UPaKQADplYFXoFAmloZCQFCQHhM4ACGwMECwkIBwUVCAkKCwUWAgMBAAAKCRBopAAOmVgVel3xEACBa6ip9yqw/7+vQtm37DgpyqI/IF/kkG9oEP1mQTYLHqOx+TAj/Jlatu8quWFui5FsK+wR132d5xTfKdh4dD1LTf7dvsj+ugkx+QDwjB0d+iAcEzGiJ3E13+3z/lr6YlpDbAgFI0+lx0llCLzzU+qFPb0i3bH8RqYiTPVVnt9WJdrlHU5KDKfCdpzgsq1WIx/9vXMfMYklPAjCVTd9nWie5qe+PCDO0Kzh++9/Z68IeWc1wq95HVD+dBcyHJuXX45Hq+la8v2stulBj/NLc9ztUOnpT4WhnjdyGqGKj3KrNYlvdtrEin35TPeWTxsG1m5MWWnJOpjf0z5jZCAqf/+fOxfFsV97PLi+hoMhI56IdXCJtoZ8cw/1k1MKrvwojuVVrULyRGRACn+rCl8wMmZe1QeZz3fuJVa3IsyZswum8aa9Y9TNwQcbw6DmnlFDD+qcJH4JPs0tlr83pn4JTkTt/tfGTl6qnNlNZHIWmVHV0E7mn0xuJI7sjtHnXSKnCJ6UlUynAZ/fzu9JALA5a7olNlGcxTuTOBnb9wkDHlRGBI8pnuJuu44AlAN0Le/Z9S9fPC1cXkEExFrNaq0+LIOyCzPQx/Lp1A/+0wz3SgKFxZ96pqgf1agPDrF/+xJNjbYCW7CKd0H4CvLzyI9Z06PEMrO7yMcgVNFXpLHFC/YJYM7BTQRpaGQlARAA5R5ktQIK10iaVFc6PJwAZKUwWgra22c6a9Umh
OWj8niMX1uzghNf8Z1lNyrsABHopymmr/F0nD5NXyJJ3+D9s7JUGR0FMiinG8PgC45ol+ejvXtCzG7/0Egv/qWYJxSHibtOy5Nmu+jFaOzGkEOfBoPAj6VfSaqPX8mpbRmvO9/XmGvKNYAnXfUOz7IqOv9gSYv5rp2B0mnOAort8TvYhe9QLcqoE/e2KzwS1xMYV+sOk9GUYSwjZJdVXK+m41sck6VVr9gu2KPIDZXpSGbj0ntH+FqPhrE/nIHGRymMP7fMW/3YKXKz0ZxgS4/p6r0Zc9uCHe3PpvPIvE4THXA7bYM2WVVvh7yPt/sAaacxPE4q1MMVRzyaOjve8IpclxFFYc9PJsqzilC6QEODjyDqycOejnDtaz3n++run8fXX2glwVgPPtAO0jiQFzxKBgtQnLpPqjlsrIorOcyvKhvRf4BsuNhjelFp7nlCQ6aWTVaeIBkUR5qx4syvS/0PQ+1/85l4QegO/j5RyYSkBnxfW5tf+ZL70wGBUy9y6fI3YHh3lNhtLciax10+acaYPqHbZYBJ3JRp6ETsrOcvZOljLvOhcC4E0NRHx375RKS/WfnRMinIwyOBLW0+vs34BDmtOctQ+UfzUXrI8Nw5h96eTU5vvCZKk3TTsrtZ/YLmlQ0AEQEAAcLBfAQYAQgAJhYhBDY9fbTsE92ymg9FD2ikAA6ZWBV6BQJpaGQl

BQkB4TOAAhsMAAoJEGikAA6ZWBV6JQ0P/0lgHVxE4y0vtg73BdeGxQZtxuK5he
Xh
uIFU2cbb1PhnlLLptfqw3f6QSpIDsBkrP0v+BRuigZFgOGicr6NzLXV2U4JccSZO
qiWtgG7FN40jugHqKGzGz7hyldcfdEsB2IDV0R8zu4HvX+6JeeSsqUNITw9AciQI
ZenRoWmCefyQc9KpQz6hvY5IbgQOxZWTuBcjuCFb/y7TPHBBlYPh8ERYfVLAKF
yh
9gOe/H6Rz52LR5omZQJHoX4/CH2OychtuKYhDB6HDyX00Fd6kaVYc7Pz3jcFp2b
d
PHKmzPJiyOeFevMN/Azr8rZVXOmomMmyqU3EwuwwDQjtN838jhgxVa4CCHND6
i7c
clR19vvm5TCTIpQua7KEsYVBvhLlsSmT5zQuyuOkdCv9Ua38Q418E4mEmWd120
C8
qm0sMwinuU52W6rvkxcciXFR3KFO/aGUQ8CHazorw+KFsio1amWnxKqf7Sx1zPe/
375YUcfMw44VIcsgWBFMZtzP8y1oOuu7DWtORAbPNOqu2l9/Cvj5TLgEtSRnbfDc
Nz0UC6tikl+KFkkuauorfCSpw/zQGdA63VfD4R+MHHAphVd77T835A9jJI43hfny
adQHWXXch3GIVOALhfuelRp1G1+vLdEJdXj0Ly+e9ZkNKJtfjRNf323OxHbSzgng
hsKULCVH4TGv
=qfSB
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
vncoolid.com

2.9. Anggota Tim

Ketua VNCOOL-CSIRT adalah MANAGER. Untuk anggota tim merujuk kepada Surat Keputusan KEPALA TIM TEKNOLOGI INFORMASI DAN SISTEM (TTIS) Nomor SK/001/VN-TTIS/2025 Tentang PEMBENTUKAN TIM TANGGAP INSIDEN SIBER (COMPUTER SECURITY INCIDENT RESPONSE TEAM - CSIRT) VNCOOL-CSIRT (VNCOOL-CSIRT)

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak VNCOOL-CSIRT

Metode yang disarankan untuk menghubungi VNCOOL-CSIRT adalah melalui *e-mail* pada alamat vncool-csirt@vncoolid.com

atau melalui nomor telepon +62 821 4567 5280
ke CATHERINE ANGELIA PERMANA pada hari kerja Senin- Jumat, 24 jam

3. Mengenai VNCOOL-CSIRT

3.1. Visi

Visi VNCOOL-CSIRT adalah Mewujudkan lingkungan siber VNCOOL-CSIRT yang aman, tangguh, dan terpercaya guna mendukung keberlangsungan bisnis serta menjaga kepercayaan seluruh pemangku kVNCOOL- CSIRT memiliki kewenangan penuh atas seluruh konstituennya (unit kerjadi lingkungan VNCOOL-epentingan.

3.2. Misi

Misi dari VNCOOL-CSIRT, yaitu :

Menyediakan layanan respons insiden siber yang cepat, efektif, dan terkoordinasi untuk melindungi sistem, data, dan layanan digital PT Vncool Teknologi Indonesia, serta meningkatkan ketahanan siber perusahaan melalui pencegahan, deteksi, dan penanganan insiden secara berkelanjutan

3.3. Konstituen

Konstituen VNCOOL-CSIRT meliputi :

a. Pencegahan & Deteksi: Menyelenggarakan sistem pemantauan keamanan siber yang proaktif untuk mendeteksi ancaman dan kerentanan sedini mungkin.
b. Penanganan Insiden: Melakukan penanggulangan dan pemulihan insiden siber secara cepat, tepat, dan efisien untuk meminimalkan dampak kerugian perusahaan.
c. Peningkatan Kapabilitas: Mengembangkan kompetensi sumber daya manusia dan teknologi keamanan informasi secara berkelanjutan.
d. Budaya Keamanan: Meningkatkan kesadaran keamanan informasi (Security Awareness) bagi seluruh karyawan VNCOOL-CSIRT.
e. Kolaborasi: Membangun kerjasama aktif dengan BSSN (National-CSIRT) dan komunitas keamanan siber lainnya dalam pertukaran informasi ancaman.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan VNCOOL-CSIRT bersumber dari dana perusahaan.

3.5. Otoritas

Vncool-CSIRT memiliki otoritas berdasarkan Surat Keputusan Manajemen PT Vncool Teknologi Indonesia untuk melakukan koordinasi, investigasi, analisis,

mitigasi, serta pelaporan insiden siber yang berdampak pada sistem, layanan, dan data perusahaan. Tim menerima otoritas penuh dari manajemen untuk berkoordinasi dengan seluruh unit kerja dan mitra terkait dalam rangka pelaksanaan tugas penanganan insiden siber

4. Kebijakan – Kebijakan

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

VNCOOL-CSIRT melayani penanganan insiden siber dengan jenis berikut:

a. Web Defacement (Perubahan tampilan situs web resmi perusahaan secara ilegal/tanpa izin).

b. Malicious Code (Malware/Ransomware) (Infeksi virus, worm, trojan, atau ransomware yang mengunci data atau merusak sistem perusahaan).

c. Denial of Service (DoS/DDoS) (Serangan yang membanjiri jaringan sehingga layanan/website perusahaan menjadi lambat atau tidak bisa diakses).

d. Phishing & Social Engineering (Upaya penipuan melalui email atau media lain untuk mencuri kredensial/password karyawan).

e. Unauthorized Access (Akses Ilegal) (Percobaan masuk ke dalam server, aplikasi, atau akun sistem tanpa hak akses yang sah).

f. Information Leakage (Kebocoran Data) (Terbukanya data rahasia perusahaan atau data pribadi pelanggan ke pihak yang tidak berwenang).

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

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

VNCOOL-CSIRT melakukan kerja sama dan koordinasi aktif dengan Badan Siber dan Sandi Negara (BSSN) selaku National-CSIRT Indonesia. Selain itu, kami juga menjalin komunikasi dengan penyedia layanan internet (ISP), vendor teknologi, serta tim tanggap insiden siber lainnya jika diperlukan dalam penanganan insiden.

Dalam hal pengungkapan informasi, VNCOOL-CSIRT menerapkan standar Traffic Light Protocol (TLP) untuk mengklasifikasikan tingkat kerahasiaan informasi. Seluruh informasi sensitif yang diterima dari pelapor atau pihak ketiga akan dijaga

kerahasiaannya dan hanya diungkapkan kepada pihak yang berwenang berdasarkan prinsip need-to-know (hanya kepada yang berkepentingan).

VNCOOL-CSIRT menjamin tidak akan mempublikasikan data pribadi, log sistem, atau rahasia dagang perusahaan kepada publik tanpa persetujuan tertulis dari manajemen atau kecuali diwajibkan oleh peraturan perundang-undangan yang berlaku.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi bersifat biasa (pertanyaan umum atau koordinasi non-teknis), dapat menggunakan e-mail: vncool-csirt@vncoolid.com dan telepon kantor di nomor +62821-4567-5280

Namun, untuk komunikasi yang memuat informasi sensitif, terbatas, atau rahasia (seperti laporan insiden, log server, atau bukti serangan), WAJIB menggunakan fitur enkripsi PGP (Pretty Good Privacy) pada e-mail untuk menjamin keamanan data.

Kunci Publik (Public Key) PGP milik VNCOOL-CSIRT dapat diunduh pada bagian Lampiran dokumen ini atau diminta melalui e-mail.

5. Layanan

5.1. Layanan Utama

Layanan utama dari VNCOOL-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini bertujuan untuk menyebarluaskan informasi mengenai potensi ancaman keamanan siber, kerentanan sistem (vulnerability), serta peringatan dini akan serangan siber yang sedang aktif kepada seluruh konstituen di lingkungan VNCOOL-CSIRT.

Peringatan yang diberikan mencakup: 1. Informasi ciri-ciri serangan (Indicators of Compromise) yang sedang marak. 2. Informasi kerentanan kritis pada perangkat lunak atau perangkat keras beserta rekomendasi pembaruan (patch). 3. Himbauan keamanan terkait isu global atau nasional yang bersumber dari BSSN (Nat-CSIRT) maupun vendor keamanan.

Peringatan ini akan didistribusikan melalui sarana komunikasi internal seperti E-mail Blast, Grup Pesan Instan Perusahaan, atau Portal Internal, dengan prioritas berdasarkan tingkat urgensi ancaman.

5.1.2. Penanganan Insiden Siber

Layanan penanganan insiden siber meliputi kegiatan koordinasi, analisis teknis, penanggulangan, serta pemulihan sistem yang terdampak oleh aktivitas ilegal atau anomali keamanan siber.

Mekanisme layanan ini dilaksanakan melalui tahapan sebagai berikut:

1. Triase (Pemilahan): VNCOOL-CSIRT akan memverifikasi validitas setiap laporan yang masuk, menentukan klasifikasi jenis insiden, serta menetapkan tingkat prioritas penanganan (Critical, High, Medium, atau Low).

2. Koordinasi Penanganan: VNCOOL-CSIRT bertindak sebagai pusat komando yang mengoordinasikan unit kerja internal (IT, Legal, HR) maupun pihak eksternal terkait untuk merespons insiden secara terpadu.

3. Resolusi Insiden: Tim akan memberikan panduan teknis atau melakukan intervensi langsung untuk mengisolasi sistem (containment), menghapus ancaman (eradication), dan memulihkan layanan (recovery) agar kembali beroperasi normal.

5.1.3. Penerimaan Aduan Insiden Siber

VNCOOL-CSIRT menerima aduan dan laporan insiden keamanan siber dari seluruh konstituen melalui jalur komunikasi resmi yang telah ditetapkan (sebagaimana tercantum pada poin 4.3 Dokumen ini).

Setiap aduan yang masuk akan diverifikasi dan dicatat ke dalam sistem tiket insiden. Pelapor akan menerima konfirmasi penerimaan laporan selambat-lambatnya 1x24 jam pada hari kerja.

Untuk mempercepat proses analisis dan penanganan, pelapor diharapkan menyertakan informasi pendukung sebagai berikut: 1. Foto tangkapan layar (screenshot) pesan error atau tampilan yang mencurigakan. 2. File log sistem atau contoh email phishing (jika ada). 3. Kronologi singkat kejadian (kapan mulai terjadi dan apa dampaknya). 4. Identitas dan kontak pelapor untuk keperluan konfirmasi lebih lanjut.”

5.2. Layanan Tambahan

Layanan tambahan dari VNCOOL-CSIRT yaitu :

5.2.1. Analisis Risiko Keamanan Siber

Melakukan penilaian risiko (risk assessment) secara berkala terhadap aset informasi vital perusahaan. Layanan ini bertujuan untuk mengidentifikasi ancaman, kerentanan, dan dampak potensial, serta memberikan rekomendasi kontrol keamanan yang tepat untuk menurunkan tingkat risiko ke level yang dapat diterima.

5.2.2. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Memberikan layanan konsultasi teknis dan prosedur keamanan kepada unit kerja lain di lingkungan VNCOOL-CSIRT yang sedang mengembangkan sistem atau aplikasi baru. Hal ini untuk memastikan prinsip Security by Design diterapkan dan sistem memiliki kemampuan pencatatan log (logging) yang memadai untuk keperluan investigasi di masa depan.

5.2.3. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Menyelenggarakan program edukasi berkelanjutan untuk membentuk budaya keamanan informasi yang kuat, meliputi: pelatihan keamanan dasar bagi karyawan baru, simulasi anti-phishing berkala, serta penyebaran materi edukasi (poster/artikel) mengenai praktik terbaik dalam menjaga keamanan akun dan data perusahaan.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke email : vncool-csirt@vncoolid.com dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

Segala informasi, panduan, dan rekomendasi yang diberikan oleh VNCOOL-CSIRT disediakan sebagaimana adanya tanpa jaminan dalam bentuk apa pun, baik tersurat maupun tersirat.

Meskipun setiap upaya telah dilakukan untuk memastikan keakuratan dan kelengkapan informasi pada saat dipublikasikan, VNCOOL-CSIRT tidak bertanggung jawab atas segala

kerugian, kerusakan data, atau gangguan operasional yang mungkin timbul akibat penggunaan atau penyalahgunaan informasi yang diberikan.

Konstituen disarankan untuk selalu melakukan pengujian (testing) dan verifikasi secara mandiri sebelum menerapkan rekomendasi teknis pada sistem produksi.