RFC 2350 CSIRT PT RAJAWALI NUSINDO (RN-CSIRT)

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi RN-CSIRT berdasarkan RFC 2350, yang mencakup informasi dasar mengenai RN-CSIRT, tanggung jawab tim, layanan yang diberikan, serta cara untuk menghubungi RN-CSIRT.

1.1. Tanggal Update Terakhir

Dokumen ini merupakan versi 1.0 yang diterbitkan pada tanggal 24 Maret 2025.

1.2. Daftar Distribusi untuk Pemberitahuan

Pihak-pihak yang menerima distribusi pemberitahuan RFC 2350 adalah seluruh Divisi dan Kantor Cabang PT Rajawali Nusindo.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia secara daring di: https://csirt.nusindo.co.id/rfc-2350/

1.4. Keaslian Dokumen

Dokumen ini telah ditandatangani secara fisik oleh Ketua Computer Security Incident Response Team PT Rajawali Nusindo (RN-CSIRT).

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu:

Judul : RFC 2350 CSIRT PT RAJAWALI NUSINDO (RN-CSIRT)
Versi : 1.0
Tanggal Publikasi : 24 Maret 2025
Kedaluwarsa : Dokumen ini berlaku hingga versi terbaru diterbitkan

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team PT Rajawali Nusindo
Disingkat: RN-CSIRT

2.2. Alamat

Gedung IDFOOD
Jalan Denpasar Raya Kav. DIII Kuningan, Jakarta Selatan 12950, Kuningan, Jakarta Selatan, Daerah Khusus Ibukota Jakarta

2.3. Zona Waktu

DKI Jakarta (GMT+ 07.00)

2.4. Nomor Telepon

(+62) 21-252-3820

2.5. Nomor Fax

(+62) 21-5291-4179

2.6. Telekomunikasi Lain

-

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

csirt@nusindo.co.id

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

Bits : 4096
ID : 0x46E8A0E89F01A44B
Key Fingerprint : EE3C E0BE 0A51 ABF6 7032 6B86 46E8 A0E8 9F01 A44B

Blok PGP Public Key:

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

mQINBGe8EBgBEADo8DOwZzwtKZJWxCzPjQhCotAbUwoEPm5D+u9gnwN8QhK4H0Kg
hbgP6b4seB3BcxCq0yzmrjEfeM7s/phek1GwoMc4tkTi5i9LLYAEg8Gw+hBByycz
7RkhN2Ebznjk8qUmuFlqV1VUt4cCIRn6waMx2qevVwrky45tC6SpSNHMAKfR8qlh
oJlGnCMIZZzVEz7Zms8XhQNPtdxjnTo9MLdKAvXAWTe5dNV6YPmk/NqgmdPkvLZw
adN5kymaZKyJjG//Df8HsdKYdI/VueK/OKyEr4XRou31Ftj14TQHWlc0N4Z+9aUJ
G9mH86QpoDzTdEkqYDNx/BMWyYXgKwVID3iXjfVn7j1lNGc70506AiJ8Wy3ZRe6q
jQPmS24AZjpjoeWWHKhcUL7ZEfh3Mhuhp+/VL2/VALW2QCMnm6fp3GdzSN8F1l64
pWEhlr+bDOs/kvOMj2nvkkIVicn1dBTNZYPFvwMfQGu3rBUtTdIGQlXeFVGoROA2
3beqrKEWHbO7RR9zj3YdPItUdGx/Ba9bK1jdSacqRMB9KxSqhwbprwJbg1N1948H
6fjZSdWKjlWenNoRBHZq69FbSi1WO2o/Ufuqhk53XZGfIfzEEkvfyEvwhy+BlJ34
kJ1XUMnWu+YLp6rf5qjdmuRTIOyccVNRLNtv8qnxs9+5Ax3VAlbMujzNGQARAQAB
tB5STi1DU0lSVCA8Y3NpcnRAbnVzaW5kby5jby5pZD6JAlcEEwEIAEEWIQTuPOC+
ClGr9nAya4ZG6KDonwGkSwUCZ7wQGAIbAwUJBaOHOAULCQgHAgIiAgYVCgkICwIE
FgIDAQIeBwIXgAAKCRBG6KDonwGkS24QD/9r7DGssz0fCm05e4D7JJUsF24i3B0l
X3QOEux4fuj3AqtdZN45UZQtx4UJQ5mdOAvkurL8XYsGsff0gPx7XQOxZi/sf8lA
EZyst+HZODTb+JHRBK+yJ8qPxL3W7OiV8a2pErhIExIQr7qXmLdkySqMrmYyWwXT
EYr831BaxDeBxZJc71P+uQEXZc12GEgGgR6xTDeWY+M6hvu0wbfORaINS0aiKeR7
95IbuYyXYVNDGWNX0RZYYFRixqUQzCveKitsl7L/xbk0VfWT7GqDwJjIpxppK3bY
EvzZse8N9ynC98DHGtCNM+UEJWzMQvhcKOdIqwshd3CrzS0zZrMILb4sgf0yqTAm
65LSUhKT9nvBI8x93P2U8lrYqVhetEEJJySOiC8JVqqpTSf64cJI4VqPYcb9A8Zw
ntv2VW2tcu6cR7lKSDVdPlvvUZ2b0/47yCHarOSay94gV1Fxxdt+MN7+gaD2j1lX
GjmSlyKWFGDe852ZbEcctiQ4cQsFU7k46mprGM9QDVg8kuqOPZ0i+t6ORc5xh2fF
GR81Rr1SfLV7JZKewmWg7QxluyCqIQc+xqpDKZTebEeLnINv7lCzNWMTtSL76pfp
AZRWU2LXiF5qpuU0VG+u0/01Y9QhV5ik09LMIOii7pl0dFwcRlU30An5a6jehrgL
1LfO+AwhQ8zxU7kCDQRnvBAYARAA3dLDn8e6pvihi32R4GURt0AuhKtkmRpfgr1a
hVM5jOiJo88PqF1QsXnlOGApxjHDyZOMGPegwoopBUFZgS/L5nk0zYRRIOzp6vkm
NAte1sGrjy2HUnhAf8JOp0rvS8UDFSH4DqAlFM83+MeHMW69Xm61dlYlG+gbRJBp
WarJkn2l1U0qt+cOFOcz4x2w0VkrOL8+31GOAwkfcoUHaAdDV7FvYIxeLSpx8I4J
8rHpsmD2pdtwsMl/8tm1vh/VlXtGtufgR5c/lmNPzGGNx6OOc846EgQkl29FlfJ0

lE3jZbcAz3owdG53EzVeD69oaoU6Aalrwtf1kKlQ3o4Y8z6F+QkY9qyUuH27UDfj
MqOEqpqXgaZ2qzz0D8hygn/DP7K75oretbdpkyhUlSAHQTPrBKgVCvrFaB5x3F00
mjq5zPHZwp+gAqhZHPyACHbF0p64P+lVZpc4czKP6ylEkf34QUaTOdZgD5IUf2GD
2LWeL0YGHlkCwSupPDaN1s8s0Y4/TjWaNICLYOgLn41DXk4kya3HhlvwIruSe6JB
GoqQkH6NLuNU4y4SJcpg5Ev+Zs61yV9iBmNvt/+tPCz7w7mAq9jDtaen1FGrU/VK
dfZPvSkDOh/iLU5j1T4ZVbFhSLz09i7TPD6mTqbsrITHWwTRhRAmUgHLWF2HFBsJ
kPwpuEUAEQEAAYkCPAQYAQgAJhYhBO484L4KUav2cDJrhkbooOifAaRLBQJnvBAY
AhsMBQkFo4c4AAoJEEbooOifAaRLL3YQANDINwg5ls09XJY2MpP5OpRTe5XKSwwU
RZPG65LJGfQQQePGDAR7B3iSXt9ykWxlBUONbAqhGcGkCn6OFF99mr6MNmwoM66C
8pQJvH66PK64lLocpXplUzGWuB8P20keG1aC5WkFCtwvrLUGkeViwSio5qPs/6vy
Y59SNmr0IrkgKMEjR43E3hwEa4TrhuVp+z9mYCSZHKoNZDQ5bdwt7b9Os2vmf0cW
38nw6FhCsQhCbzCSxI7fxTNxXXeRRu28aiAxHA7CvxfQrJ2l0IzkhDZk06nn6qbx
Ni6sbpvLtMpQmXZyXuy4wK3iwr8WE7dkjFuem7FLHWa4LBxBqsCnrkqUjZdhcOL/
r/3vcCSlWtUOlfRb7CkXM6rqQ4bPDo8/UMsjTQrHMZF/OqwqqHM0Q1+ObUfxxtnS
K66U9oFs9+rSJ9Lfb46Y3ZETqOjneKvp6kBLgvDSYDgifuz12WbtJ/N1Q6tnLtiE
cKfUvwoZ/Ol9Ivv5bIUcZk1w8lusfgfOAujSjozXjhQyQTlBzNi861FVBnqVzUk0
pj7joJ+796CcQQINScV3aEPrgho10zSISbGDZC9uJ8DPtgm0kofihBxwn+ei50t9
ASHgJFgwg5JFKTdi+abc4NZTHL5Vq/aGaNA7L2XK1BMIQmAhKwD4hQwgzU/5UhHh
ItTiIqkbdqQz
=uhC7
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia secara daring di:
https://static.nusindo.co.id/csirt/file/public_key/rn-csirt_public_key.asc

2.9. Anggota Tim

1. Pengarah: Direktur Keuangan & Pendukung Bisnis PT Rajawali Nusindo
2. Ketua: GM Akuntansi Keuangan
3. Wakil Ketua: Manajer Teknologi Informasi
4. Sekretaris dan Anggota: Staf serta Pelaksana Teknologi Informasi PT Rajawali Nusindo

Daftar susunan tim dapat dilihat dalam dokumen SK Pembentukan Computer Security Incident Response Team (CSIRT) PT Rajawali Nusindo dengan Nomor: 913/SK/Nus.01.00/XII/2024.

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak RN-CSIRT

Metode yang disarankan untuk menghubungi RN-CSIRT adalah sebagai berikut:

1. Email: csirt@nusindo.co.id
2. Halaman Aduan Siber: https://csirt.nusindo.co.id/layanan/aduan-siber/
3. Telepon: (+62) 21-252-3820 (Hari kerja, pukul 08.00 - 17.00 WIB)

3. Mengenai RN-CSIRT

3.1. Visi

Visi RN-CSIRT adalah Menjadi tim respons keamanan terdepan dalam melindungi integritas, kerahasiaan, dan ketersediaan informasi guna mendukung keberlangsungan dan inovasi bisnis perusahaan.

3.2. Misi

Misi dari RN-CSIRT, yaitu:

1. Mendeteksi, merespons, dan memitigasi insiden keamanan informasi dengan cepat, akurat, dan efektif.
2. Mengkoordinasikan upaya pencegahan, penanggulangan, serta pemulihan insiden keamanan siber di seluruh organisasi.
3. Membangun budaya keamanan siber melalui edukasi, penerapan keamanan informasi, dan peningkatan kesadaran di seluruh organisasi.
4. Memperkuat kerja sama antar divisi, kantor cabang, serta pemangku kepentingan internal dan eksternal untuk meningkatkan ketahanan terhadap ancaman siber.
5. Mengembangkan solusi inovatif dan berkelanjutan guna meningkatkan kapabilitas pertahanan siber perusahaan.

3.3. Konstituen

Konstituen terdiri dari seluruh divisi dan kantor cabang PT Rajawali Nusindo.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan RN-CSIRT bersumber dari Anggaran Perusahaan PT Rajawali Nusindo.

3.5. Otoritas

Otoritas dari RN-CSIRT adalah sebagai berikut:

1. Bertanggung jawab kepada Direksi PT Rajawali Nusindo.
2. Wajib menyampaikan laporan secara berkala kepada Direksi PT Rajawali Nusindo terkait setiap pelaksanaan tugas.
3. Berkoordinasi dengan Kantor Cabang PT Rajawali Nusindo terkait dengan penanganan insiden siber.

4. Kebijakan – Kebijakan

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

RN-CSIRT menangani insiden keamanan informasi yang terjadi di berbagai Unit Kerja, Divisi, dan Kantor Cabang PT Rajawali Nusindo. Layanan diberikan berdasarkan laporan konstituen, dengan skema sebagai berikut:

1. Tim layanan bantuan menangani insiden di level Unit Kerja.
2. Jika insiden tidak dapat diselesaikan oleh tim layanan bantuan, maka akan dieskalasikan ke RN-CSIRT.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

RN-CSIRT melakukan kerja sama, koordinasi, dan berbagi informasi dengan Nat-CSIRT atau organisasi sektoral lainnya di bidang keamanan siber. Seluruh informasi terkait insiden siber yang diterima oleh RN-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

1. Komunikasi umum dapat dilakukan melalui email tanpa enkripsi (email konvensional), halaman Aduan Siber, atau telepon.
2. Komunikasi yang bersifat sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP (opsional) melalui email.

5. Layanan

5.1. Layanan Utama

Layanan utama dari RN-CSIRT mencakup pemberian peringatan terkait keamanan siber serta penanganan insiden siber, dengan rincian sebagai berikut:

5.1.1. Pemberian peringatan terkait keamanan siber

a. Memberikan informasi mengenai potensi ancaman dan risiko keamanan siber.

b. Menyediakan literasi keamanan informasi bagi konstituen.

5.1.2. Penanganan insiden siber

5.1.2.1 Triase Insiden

a. Menerima dan mencatat laporan insiden dari konstituen.

b. Memverifikasi validitas insiden serta mengidentifikasi identitas pelapor.

c. Menilai tingkat keparahan, dampak, dan prioritas insiden untuk langkah penanganan lebih lanjut.

5.1.2.2 Reaktif Insiden

a. Melakukan koordinasi dengan pihak terkait dalam penanganan insiden.

b. Menyampaikan laporan insiden kepada Direksi dan Komisaris, termasuk langkah-langkah yang telah diambil.

5.1.2.3 Koordinasi Insiden

a. Berkoordinasi dengan konstituen dalam proses penanganan insiden.

b. Memberikan rekomendasi berdasarkan SOP dan panduan RN-CSIRT.

c. Mengkoordinasikan insiden dengan CSIRT terkait lainnya.

5.2. Layanan Tambahan

Layanan tambahan dari RN-CSIRT mencakup:

5.2.1. Penanganan kerawanan sistem elektronik

a. Mengidentifikasi dan menilai kerentanan dalam sistem elektronik.

b. Memberikan rekomendasi mitigasi terhadap celah keamanan yang ditemukan.

5.2.2. Pendeteksian serangan

a. Menggunakan sistem deteksi ancaman untuk memantau aktivitas yang mencurigakan.

b. Mengidentifikasi pola serangan yang dapat membahayakan sistem organisasi.

5.2.3. Konsultasi terkait kesiapan penanganan insiden siber

a. Menyediakan layanan konsultasi bagi konstituen terkait kesiapan dalam menangani insiden siber.

b. Membantu organisasi dalam menyusun prosedur respons insiden yang efektif.

5.2.4. Pembangunan kesadaran dan kepedulian terhadap keamanan siber

a. Mengadakan pelatihan dan sosialisasi tentang keamanan siber.

b. Meningkatkan budaya keamanan informasi di seluruh organisasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan melalui email ke csirt@nusindo.co.id dengan melampirkan sekurang-kurangnya:

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

7. *Disclaimer*

-