PT. ALTO Network
Head Office
Menara BCA Grand Indonesia Lt36
Jl. MH Thamrin No.1, Menteng,
Jakarta Pusat, Indonesia, 10310
Telp : 62-21 5055 8600

RFC 2350 CSIRT Alto Network

1. Informasi Mengenai Dokumen:

Dokumen ini berisi deskripsi CSIRT Alto Network berdasarkan RFC 2350, yaitu informasi dasar mengenai CSIRT Alto Network, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi CSIRT Alto network melalui email csirt@alto.id.

a. Tanggal Update Terakhir : Dokumen merupakan dokumen versi 1.0

b. Daftar Distribusi untuk Pemberitahuan : Tidak ada daftar distribusi untuk pemberitahuan pembaharuan dokumen.

c. Lokasi Document Tersedia : https://github.com/altonetworksecurity/csirt

d. Keaslian Dokumen : Dokumen asli terdapat 2 jenis, berbahasa Indonesia, berbahasa Inggris. kedua dokumen telah ditanda tangani dengan PGP Key milik CSIRT Alto Network. Untuk lebih jelas dapat dilihat pada Subbab 2.f

e. Identifikasi Dokumen yang memiliki atribut, sebagai berikut :

Title	RFC 2350
Version	1.0
Document Date	1 May 2024
Expiration	This document is valid until superseded by a later version

2. Informasi Data/Kontak

a. Nama Tim

Kepanjangan dari	Cyber Security Incident Response – Alto Network
DisingkaT	CSIRT – Alto Network

b. Alamat :
Blok C4 No.5, Satrio Tower Building, Jl. Prof. DR. Satrio 12th floor, Kuningan, Jakarta, Daerah Khusus Ibukota Jakarta 12950.

c. Zona Waktu :
Jakarta, Indonesia (GMT+7)

d. Nomor Telepon
+62 21 5085 8600

e. Alamat Surat Elektronik (E-mail)
csirt@alto.id

f. Kunci Publik (Public Key) dan Informasi/Data Enkripsi lain
Kami menggunakan PGP untuk pertukaran informasi (pemberitahuan, pelaporan insiden, dll.) dengan rekan, mitra, dan konstituen.

Bits	EdDSA (Sign only) - ed25519
Key ID	95ED2B77B69F0833
Key Fingerprint	BC19 9884 47BC DC7C 3EC2 C255 95ED 2B77 B69F 0833
Blok PGP	-----BEGIN PGP PUBLIC KEY BLOCK----- xjMEZpngvBYJKwYBBAHaRw8BAQdA+T4czaV2fb931o75fgJk5fVSF2XeNDHy TiN2j3rTv1PNJENTSVJUIC0gQWx0byBOZXR3b3JrIDxjc2lydEBhbHRvLmlk PsKMBBAWCgA+BYJmmeC8BAsJBwgJkJXtK3e2nwgzAxUICgQWAAIBAhkBApsD Ah4BFiEEvBmYhEe83Hw+wsJVle0rd7afCDMAANEeAP0TXPFfYWdq/0FRn0M6 Ur9/kh31cURibKS3aLFyzfBeVgEA6fj0n22ahiuaJc2i3r//vjKKNdnvQtkm bvxVgasmHAPOOARmmeC8EgorBgEEAZdVAQUBAQdA5JIwo+VNpCeek7p9PYYJ nzZOipGE4Teo49+b0uP+tVUDAQgHwngEGBYKACoFgmaZ4LwJkJXtK3e2nwgz ApsMFiEEvBmYhEe83Hw+wsJVle0rd7afCDMAAEC1AQDQuZfSZsHiViJ2DuOn woLu/TwOE3uEg5eBzJYeMpmRFAEAitys51xfLCJtUmXWS74lGvOl63wRiXow UgVZRoK3SQQ= =spRA -----END PGP PUBLIC KEY BLOCK-----

g. Anggota Tim
Ketua CSIRT – Alto Network adalah Rionaldo Palinggi , yang dibantu oleh tim yang terdiri dari 30 anggota staf.

h. Catatan-catatan pada Kontak CSIRT – Alto Network
Metode yang disarankan untuk menghubungi CSIRT – Alto Network adalah melalui e-mail pada alamat csirt@alto.id atau melalui nomor telepon +62 21 5085 8600 yang siaga selama 24 H.

3. Mengenai CSIRT – Alto Network

a. Visi & Misi

Visi :

Meningkatkan pengalaman pembayaran digital yang aman melalui peningkatan keamanan data dan siber.

Misi :
Misi dari CSIRT – Alto Network , yaitu :

- Memberikan pelayanan yang aman dalam penerapan teknologi pembayaraan digital yang bertujuan terbentuknya ketahanan dan kehandalan siber yang menunjang tujuan bisnis
- Memberikan Edukasi dan kesadaran siber pada karyawan dan pengguna jasa teknologi pembayaran Alto dengan tujuan meningkatkan ketahanan siber.
- Memberikan informasi temuan kerentanan, potensi serangan serta informasi tentang intelijen siber lainnya yang bertujuan agar terbentuknya ekosistem ketahanan siber baik di dalam atau pun di luar alto.

b. Konstituen

Konstituen CSIRT – Alto - Network meliputi :

- PT Nova Digital Perkasa

c. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT – Alto Network bersumber dari internal Alto – Network.

d. Otoritas

- Menentukan assesmen tingkat keamanan informasi pada proses bisnis yang sedang atau yang akan berlangsung.
- Melakukan asesmen tingkat keamanan sistem informasi yang dibuat secara sendiri (in-house), atau disewa/dibeli ke pihak ketiga.
- Melakukan pengawasan serta intervensi aktif terhadap operasional sistem informasi dalam rangka pemenuhan ketahanan dan keandalan siber yang menunjang tujuan bisnis.
- Merencanakan, membuat dan mengoperasikan rancang bangun mekanisme pertahanan berlapis siber (cyber defense-in-depth).
- Melaksanakan program kesadaran keamanan siber bersama stakeholder terkait.
- Memiliki otoritas penuh untuk melaksanakan koordinasi dan intervensi internal dan eksternal, akses terhadap data dan sistem dalam hal penanganan insiden siber.

4. Kebijakan – Kebijakan

a. Jenis-jenis Insiden dan Tingkat/Level Dukungan
CSIRT – Alto Network melayani penanganan insiden siber dengan jenis berikut :

Layanan utama :

- Pemberian peringatan terkait keamanan siber
- Penanganan insiden siber

Layanan tambahan :

- Penanganan kerawanan sistem elektronik pembayaran
- Penanganan artefak digital
- Pemberitahuan hasil pengamatan potensi ancaman
- Pendeteksian serangan
- Analisis risiko keamanan siber
- Konsultasi terkait kesiapan penanganan insiden siber
- Pembangunan kesadaran dan kepedulian terhadap keamanan siber

b. Kerja sama, Interaksi dan Pengungkapan Informasi/data

CSIRT – Alto Network akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CSIRT – Alto Network akan dirahasiakan.

c. Komunikasi dan Autentikasi

Untuk komunikasi bersifat biasa atau bukan data yang bersifat sensitif/terbatas/rahasia ke CSIRT – Alto Network dapat menggunakan e-mail tanpa enkripsi data khusus (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP/RSA (Encryption PGP Alto - sub-bab 2.f) pada e-mail atau lampiran email.

5. Layanan

Layanan utama dari CSIRT Alto – network yaitu :

a. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini akan dilaksanakan oleh CSIRT – Alto Network yang berupa peringatan akan adanya ancaman siber kepada pemilik/penyelenggara financial service tidak terbatas pada PIP dan PJP.

b. Penanganan Insiden Siber

Layanan penanganan insiden siber mencakup siklus penuh penanganan insiden. Penanganan dapat dilaksanakan dengan on-site secara langsung atau pemberian saran penanganan untuk ditindaklanjuti.

c. Layanan tambahan dari CSIRT Alto - Network yaitu :

Penanganan Kerawanan Sistem Elektronik
Layanan ini berupa koordinasi, analisis dan rekomendasi teknis dalam rangka penguatan aspek kendali keamanan (security control) baik dalam lingkup teknis ataupun non-teknis (Policy/Governance). Secara umum penanganan ini dibagi menjadi :

- Pelaporan kerawanan yang bersifat sewaktu oleh pemilik/penyelenggara sistem elektronik milik konstituen.
- Layanan penanganan kerawanan sebagai tindak lanjut dari kegiatan audit atau vulnerability assessment.

d. Penanganan Artefak Digital

Layanan penanganan artefak digital dilakukan dalam rangka menjaga sebaik mungkin proses chain-of-custody yang mungkin diperlukan dalam rangka penyidikan oleh penegak hukum atau sebagai sarana investigasi teknis insiden.

e. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan dari hasil pengamatan oleh fungsi intelijen siber milik CSIRT Alto-Netwok terhadap aset digital milik konstituen.

f. Pendeteksian Serangan

Layanan ini diberikan apabila CSIRT Alto - Network memiliki visibilitas atas sistem keamanan yang diterapkan oleh konstituen, serangan pada konstituen akan dikorelasikan untuk memperkuat postur secara keseluruhan.

g. Analisis Risiko Keamanan Siber

Layanan ini diberikan dengan tujuan sebagai fungsi perkiraan terhadap attack surface milik konstituen, layanan ini diberikan secara berkala sesuai dengan periode audit kepatuhan.

h. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Layanan konsultasi ini diberikan dalam rangka membantu para konstituen agar memiliki kesiapan yang cukup dalam menghadapi insiden siber.

i. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Layanan ini diberikan kepada konstituen dalam rangka membangun *people-process-technology* untuk menunjang program edukasi kesadaran keamanan informasi yang berkelanjutan.

j. Pelaporan Insiden

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

- Informasi: Nama Lengkap, Jabatan, No HP dan Konstituen asal.
- Bukti insiden berupa foto atau screenshoot atau log file yang ditemukan.
- Bukti atau informasi lain sesuai dengan kebutuhan penanganan insiden sesuai ketentuan yang berlaku.
- Jika Bukti incident bersifat rahasia maka di lakukan penerapan encryption metode PGP menggunakan kunci-publik pada point 2.f.

6. Disclaimer

a. CSIRT Alto-Network melaksanakan kegiatan respon insiden dengan menerapkan prinsip kerahasiaan sebagai prinsip kerja, pembagian informasi ke para pihak akan dilakukan dengan menerapkan prinsip need-to-know.

b. CSIRT Alto-Network menyediakan layanan konsultasi dengan lingkup terbatas dengan tujuan ketahanan siber bersama dengan usaha semaksimal mungkin, kami tidak dapat menjamin hasil akhir secara pasti dari pekerjaan yang tercantum pada daftar layanan.

c. Kami tidak bertanggung jawab atas kebenaran dan/atau kecepatan dari laporan terkait diseminasi informasi ancaman.

d. CSIRT Alto-Network hanya menyediakan sarana komunikasi melalui kanal yang tercantum pada RFC2350, kami tidak bertanggung jawab atas komunikasi yang mengatasnamakan CSIRT Alto-Network melalui kanal lain.