RFC 2350 CSIRT-AFI

1. Informasi Mengenai Dokumen

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

1.1. Tanggal *Update* Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 20 Mei 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Internal CSIRT, Internal Divisi TI, dan BSSN

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://akulakufinance.co.id/csirt/

1.4. Keaslian Dokumen

Dokumen RFC 2350 ini telah ditandatangani secara langsung/fisik oleh Head of IT Governance & Security PT Akulaku Finance Indonesia sebagai Koordinator CSIRT

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 CSIRT-AFI;
Versi	: 1.0;
Tanggal Publikasi	: 20 Mei 2026;
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Cyber Security Incident Response Team - Akulaku Finance Indonesia
Disingkat : CSIRT-AFI.

2.2. Alamat

Gedung Sahid Sudirman Center Lt. 11-C. Jalan Jendral Sudirman Kav. 86, Karet Tengsin, Tanah Abang, Jakarta Pusat, 10220

2.3. Zona Waktu

Asia/Jakarta (GMT+07:00)

2.4. Nomor Telepon

021 22531842

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak Ada

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

cybersecurity[at]akulakufinance[dot]co[dot]id

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

Bits : 4096
ID : 587DCC4B42FB48BD
Key Fingerprint : EBC9AE20CF4853FE8691CA53D7571E9A5D0B5D5E

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

mQINBGoeWJYBEADbjJqFO0XAitW9BgqovGtuqbECo+NsnHB+CIFI0R4u3H3c1NTJ
0CLpkZz832cryTi3ynDZZ329x8a0W/xykZZxWxzRMvm3SahpGpF89FOnwkvR1Zre
G6WCVR/10n7kWf0oXqf3uHyKF7tN7DlU1J7iku5ymBhEAY0XTuKEHh5TXcOSVNSx
iKaAqRoRCe57V6NeXR7Mr7IvcrY08oEIEp7zVt5WDbRKx8VBvHw3S7IIva8KkbUA
zGNzwg9Ea87wIRl6nZyp6BhImoE2iUy0WmoIpx37TGHoxEM0cQ621KbLU6hdvMaZ
kdPq4Bt0izeT/37+InquYSmmWOQDbKy8ejSf3wbuISFyWK6WZ70+x3IdJBMkLm20
XyEfevRNp3PYWJIsh9E4f8DOOHRefcYvAi9kqWopgsXTLDWNUWNABB0OjFVd8xud
WBRRe5bxfXrrQ3MyqMN5/KTnvnagakCwjenQCKCdANNPnjON9kq3RVg6AR/fD2G7
SjgfJbboTkdgk3C5pqva8nJU8R8S94G8rujtUOwysfxsjOyfBi5kf/cQsGfvryjz
1CkvBitQAz9udRabTL3kSaacBjjDS20HpQueQ73rsdTReZFdJGRGs8DVO5wPX5hZ
DfhFis0X8CY74wM3AdGyVPqlpGTikPFvn2lc31NW5mtzmzGkXHSiLJdxfQARAQAB
tHVDU0lSVC1BRkkgKENvbXB1dGVyIFNlY3VyaXR5IEluY2lkZW50IFJlc3BvbnNl
IFRlYW0gLSBBa3VsYWt1IEZpbmFuY2UgSW5kb25lc2lhKSA8Y3liZXJzZWN1cml0
eUBha3VsYWt1ZmluYW5jZS5jby5pZD6JAk4EEwEKADgWIQTrya4gz0hT/oaRylPX
Vx6aXQtdXgUCah5YlgIbAwULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRDXVx6a
XQtdXvoxD/9+n0DEWvN7MdA62zBrOgDOnfdjkz8kxuaN9HBHLuG9b0/83sVh1xU5
btWlgW2h/uvoanvAuZNALqsYgyE4q0RI5KnYftSfN8+E4NB3hk1j/LYdbFFF44tf
G+KQxFTNUfl7XfZrhCgjs6yH0kTwleaBb3bf+PyC8UPQ4Euwm7eLR6kS3/S19Jti
zIcup2BpQKMcq9eu2jHbHrskTT3EagjpGhgC1EV7Cx9ICnF8G0MYPwKueasSmbcs
vGtlcNEhXCnTK1cQP12XeDDvTniiCTYJFsDMjev0GXP7B/ixFQRjzePZusHplz9+
iHvLsLsH0im4iUDWujYCwjftTbotE0p65OQ73byBQd+JOhaf+qFIqEvv/ITnK3py
bDdLjKwmFgmSHtQXmTBExeTYO4zmco8lgSgCljFFmY6/BqeRL0eWsLvnBmxk6mbN
RJMRi8qkGHlmMDmNYEfgPftRD9ige7lfjsKXSllyzveqZYrkQoT6KjMB3ktzlVeF
fa7jbnEm3eh8D8m3gwrc6z3mIU0Ut0/vSryOlXEiz6++XBybhvF+OEXQQFjsRjOO
te9WE3rxd9+61J0TCUVlFE+Su7sCTEi2EJ5jSy5K/aXR8qLNWvb9qF7iv4SUfDXP
fAOtL7V7sSzikFbc218BF7Bf2MnhCXzqMORTYviE2ZFwWUKcOS9wQ7kCDQRqHliW
ARAA4GxT9RnfsXoUA7Fm8p3w67TZOCG/V+BUwNcF3XGpq83tco/beOb5OksfYed4
okcz7zCHehqpbkMaLR914wVfALZUpdGcRX8PW/PErA37X4layKPL9g/TUDaQ0hGC
WlBOmAhwU7+CDiD90w2O3CNUQ1RFxiKLE+o8fWDbbHXWirmDFN7acmdqPaChxOrl
sphjDz3egwrOem84jNkGZPUyPiCxf4UlyRnssTuDxou9ltdvdhke/om5kQcwUTmV
1nGo6UUmEkIXR0ChSNuzIQ/ho0I8T/OWys3Q4KuA6SW3KpE5GO0dRqL6OcrEQYmv
SAqeVz24PUBugHUXIVuqLq8xqwP8O/WqHE9+IxKkL/0MhkqMi7GasiJbhq6WIIQW
GvYi9HNmHgztOkodgfkpxFQch6z7O8/yv/8gJnJV8PjbqwNkg7b6qQQZw64H94lf
JB9y8i8XeFa+zmXU28zYAu+2ldnYVy2WfwfXdX5HFhBrjbbhn6dQvlmVNv7Dp31/
d0EqH4w6dBaVnBlfzSdBG47fYwRPRhoIdCHUxAldL/bWDgf+KcPgoskQaKGE7W7J
riz7U/afcGsv4m5vsyOU3a30sg0pfk1gfnKQTyuVkv0VfAAYsWlH/9g83o2uqTKu
N78jMpy+jqEYipgBuqTY3/xdOwd3paWEqsv50Tl5j9jvEukAEQEAAYkCNgQYAQoA
IBYhBOvJriDPSFP+hpHKU9dXHppdC11eBQJqHliWAhsMAAoJENdXHppdC11evgkQ
AIlhwTYblMINY74vQSepUtCzQ8zB6RH3VdN1KpTQ5vRZGUsKnfxPdHd3xPFcWls8
k4uKNsJxHJtArp9bNl9g7LpiOSlJYXQYOdKi7p1SlZi5aP51+RBved11P9uJECmw
9sNeKjL3FPEImMFUMser/4EF9kvN8bgUxMp5zGgmdgyn8+sOh9mZ38njdPR59r4J

08TTGrmAXrEZAtaoibLZdTqfRPo7ey0gChYiOYPMqstnrDo9n0GXbJZeMXz8UM5W
2ajknvhRRbI7I9w52fzStwgHeqWQGVv9mv3hRPdgBxt5Ej9+52jO4UWGvWpDgSAW
LM3LWD4at1aI8oKRi/kAdtTz4VO7u3v5SFW6tFNtE8QeZtHWWjzHcLuYkUPaXNTW
7iGLmJx8fVOYNiLufrMJKJVv0ojIAQUmNnAJdjmLbsOlsbk2XBeRdrtqm3Okxdu+
UOX9G3ylXHd/PXakm0bU+kN5kyNPUfM6ThOWuaV2npjgZwt6Qo4GGRjD6f0+R7bv
IcrwpGe0RqX4BubwTdhkDD4HvmgIQCqIZK8oGe3H2LHHaOQ4NMlrVQG4zs7l+234
EB9r143SwA0o0hk7xb6NUskULGNmO1sMyT9oP3D1P5n6eTpVaF02CD5SGrByhbhl
hZSGtdpUjm96wbioJGfuvftPP6hxmXxD/7JOMjjs8W6g
=63ma
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://akulakufinance.co.id/rfc2350_pubkey.asc

2.9. Anggota Tim

Koordinator CSIRT-AFI adalah pejabat Head of IT Governance & Security ditunjuk oleh Direksi TI. Untuk penunjukan dan anggota tim dapat merujuk ke Surat Keputusan Direksi Nomor 021/AFI/SK-DIR/CSIRT-AFI/ES/V/2026 Tentang *Computer Security Incident Response Team* PT Akulaku Finance Indonesia

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak CSIRT-AFI

Metode yang disarankan untuk menghubungi CSIRT-AFI adalah melalui *e-mail* pada alamat cybersecurity[at]akulakufinance[dot]co[dot]id.

3. Mengenai CSIRT-AFI

3.1. Visi

Visi CSRIT-AFI adalah menjadi tim respon insiden keamanan komputer yang profesional, responsif, dan terpercaya dalam melindungi aset informasi organisasi serta mendukung keberlangsungan bisnis melalui penanganan insiden siber yang efektif dan berkesinambungan..

3.2. Misi

Misi dari CSIRT-AFI, yaitu :

a. Menyelenggarakan layanan penanganan insiden keamanan siber secara cepat, terkoordinasi, dan terdokumentasi sesuai dengan prosedur yang berlaku.
b. Melaksanakan deteksi, analisis, penanggulangan, dan pemulihan insiden keamanan siber untuk meminimalkan dampak terhadap operasional organisasi.
c. Meningkatkan kemampuan kesiapsiagaan dan ketahanan siber organisasi melalui pemantauan ancaman, analisis kerentanan, dan penerapan praktik keamanan yang baik.
d. Membangun koordinasi dan kolaborasi dengan unit kerja internal, regulator, serta komunitas keamanan siber dalam rangka pertukaran informasi dan penanganan insiden.
e. Menyediakan layanan advisori dan edukasi keamanan siber untuk meningkatkan kesadaran dan budaya keamanan informasi di lingkungan organisasi.
f. Mengembangkan kompetensi personel CSIRT secara berkelanjutan melalui pelatihan, sertifikasi, simulasi, dan kegiatan peningkatan kapasitas lainnya.

g. Melaksanakan pengelolaan informasi ancaman siber (Cyber Threat Intelligence) untuk mendukung pengambilan keputusan dan langkah mitigasi yang proaktif.

3.3. Konstituen

Konstituen CSIRT-AFI adalah seluruh pengguna TI (Teknologi Informasi) di lingkungan CSIRT-AFI

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CSIRT-AFI bersumber dari anggaran TI PT Akulaku Finance Indonesia

3.5. Otoritas

Berdasarkan Surat Keputusan Direksi PT Akulaku Finance Indonesia Nomor SK 021/AFI/SK-DIR/CSIRT-AFI/ES/V/2026 Tentang Computer Security Incident Response Team (CSIRT), PT Akulaku Finance Indonesia berwenang untuk melakukan pengelolaan insiden keamanan TI secara proaktif dan reaktif.

4. Kebijakan – Kebijakan

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

CSIRT-AFI memiliki otoritas untuk menangani berbagai insiden keamanan siber yang terjadi atau mengancam konstituen dan kepentingan strategis siber, seperti namun tidak terbatas:

a. Web Defacement,
b. DDoS,
c. Malware,
d. Phishing,
e. Ransomware,
f. Akses Illegal,
g. Spam

Dukungan yang diberikan oleh CSIRT-AFI kepada konstituen dapat bervariasi sesuai dari jenis, dampak insiden, dan layanan yang digunakan.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CSIRT-AFI akan melakukan kerjasama dan berbagi informasi dengan CSIRT organisasi lainnya yang memiliki kewenangan dalam lingkup keamanan siber.
Informasi/data yang diberikan dan diterima oleh AFI-CSIRT dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi mengenai insiden keamanan siber yang tidak memuat informasi sensitif/rahasia/terbatas dapat menggunakan alamat email tanpa enkripsi data (email konvensional) dan telepon. Sedangkan untuk komunikasi yang memuat informasi sensitif/rahasia/terbatas dapat menggunakan enkripsi PGP pada email

5. Layanan

5.1. Layanan Utama

Layanan utama dari CSIRT-AFI yaitu :

5.1.1. Pemberian peringatan terkait Keamanan Siber

Menyampaikan informasi peringatan dini mengenai ancaman, kerentanan, atau potensi serangan siber yang dapat memengaruhi organisasi.

5.1.2. Perumusan panduan teknis penanganan Insiden Keamanan Siber

Menyusun dan menyediakan panduan teknis untuk mendukung proses identifikasi, penanganan, pemulihan, dan pelaporan insiden keamanan siber.

5.1.3. Pencatatan setiap laporan/aduan yang dilaporkan

Menerima, mencatat, dan mengelola setiap laporan atau aduan terkait insiden keamanan siber sebagai dasar tindak lanjut dan dokumentasi.

5.1.4. Pemberian rekomendasi langkah penanganan awal kepada pihak terdampak

Memberikan arahan dan rekomendasi mitigasi awal guna mengurangi dampak insiden sebelum penanganan lebih lanjut dilakukan.

5.1.5. Pemilahan (triage) Insiden Keamanan Siber sesuai dengan kriteria yang akan ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani

Melakukan klasifikasi dan prioritas insiden berdasarkan tingkat dampak, urgensi, dan risiko untuk menentukan penanganan yang tepat.

5.1.6. Penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan

Mengkoordinasikan proses penanganan insiden dengan pihak internal maupun eksternal yang terkait guna memastikan respons yang efektif dan terintegrasi.

5.1.7. Penyelenggaraan fungsi lainnya sesuai kebutuhan

Melaksanakan fungsi tambahan yang relevan dengan tugas dan tanggung jawab CSIRT sesuai perkembangan ancaman, kebutuhan organisasi, dan ketentuan yang berlaku.

5.2. Layanan Tambahan

Layanan tambahan dari CSIRT-AFI yaitu:

5.2.1. Penanganan kerentanan Sistem Elektronik

Memberikan dukungan dalam identifikasi, analisis, pelaporan, dan rekomendasi mitigasi terhadap kerentanan pada sistem elektronik.

5.2.2. Penanganan artefak digital

Melakukan pengumpulan, analisis, dan pengelolaan artefak digital yang berkaitan dengan insiden keamanan siber untuk mendukung proses investigasi.

5.2.3. Pemberitahuan hasil kematangan potensi ancaman

Menyampaikan hasil analisis terkait tingkat kematangan, tren, dan potensi ancaman siber yang dapat berdampak pada organisasi.

5.2.4. Pendeteksian serangan

Mendukung proses identifikasi dan deteksi aktivitas mencurigakan atau serangan siber yang menargetkan aset informasi organisasi.

5.2.5. Analisis risiko keamanan siber

Melakukan analisis risiko terhadap ancaman dan kerentanan keamanan siber guna mendukung pengambilan keputusan mitigasi yang tepat**.**

5.2.6. Konsultasi terkait kesiapan penanganan insiden siber

Memberikan konsultasi dan rekomendasi untuk meningkatkan kesiapan organisasi dalam menghadapi dan menangani insiden keamanan siber.

5.2.7. Pembangunan kesadaran dan kepedulian terhadap keamanan siber

Menyelenggarakan kegiatan edukasi, sosialisasi, dan kampanye kesadaran keamanan siber guna meningkatkan pemahaman dan budaya keamanan informasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke cybersecurity[at]akulakufinance[dot]co[id] dengan melampirkan sekurang-kurangnya :

a. Nama lengkap sesuai identitas, alamat email, dan nomor kontak yang dapat dihubungi
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

Seluruh penanganan tergantung dari ketersediaan tools yang dimiliki PT Akulaku Finance Indonesia

Jakarta, 20 Mei 2026

Head of IT Governance & Security

Alvian Sendy Anthonius